PERFORMANCE ANALYSIS OF HYBRID DECODE-AMPLIFY-FORWARD (HDAF) RELAYING FOR IMPROVING SECURITY IN COOPERATIVE WIRELESS NETWORK

A Thesis submitted in partial fulfillment of the Requirements for the degree of

Master of technology
In
Electrical Engineering
(Electronic Systems and Communication)

By

THATHA DIVYA

Roll no: 213EE1283

Department of Electrical Engineering

National Institute of Technology Rourkela

Rourkela, Odisha, 769008, India

May 2015

PERFORMANCE ANALYSIS OF HYBRID DECODE-AMPLIFY-FORWARD (HDAF) RELAYING FOR IMPROVING SECURITY IN COOPERATIVE WIRELESS NETWORK

A Thesis submitted in partial fulfillment of the Requirements for the degree of

Master of technology
In
Electrical Engineering
(Electronic Systems and Communication)

By

THATHA DIVYA

Roll no: 213EE1283

Under the Guidance of

PROF. SUSMITA DAS

Department of Electrical Engineering

National Institute of Technology Rourkela

Rourkela, Odisha, 769008, India

May 2015

Dedicated to...

My parents and my brother and sister

DEPARTMENT OF ELECTRICAL ENGINEERING
NATIONAL INSTITUTE OF TECHNOLOGY, ROURKELA
ROURKELA – 769008, ODISHA, INDIA

Certificate

This is to certify that the work in the thesis entitled **Performance Analysis of Hybrid Decode Amplify-Forward (HDAF) Relaying for Improving Security in Cooperative Wireless Networks** by **Thatha Divya** is a record of an original research work carried out by her during 2014-2015 under the requirements for the supervision and guidance in partial fulfillment of the requirements for the award of the degree of Master of Technology in Electrical Engineering (Electronic Systems and Communication), National Institute of Technology, Rourkela.

Place: NIT Rourkela

Date:29/05/2015

Prof. Susmita Das

Associate Professor

DEPARTMENT OF ELECTRICAL ENGINEERING
NATIONAL INSTITUTE OF TECHNOLOGY, ROURKELA
ROURKELA – 769008, ODISHA, INDIA

Declaration

I certify that,

(a) The work in the thesis has done by myself,under the general supervision of my supervisor.

(b) The work has not been submitted to any other institution, for any other degree or diploma.

(c) I have followed the guidelines provided by the institute in writing this thesis.

(d) Whenever I have used materials (data,theoritical analysis and text) from other sources, I have given due credit to them by citing them in the text of the thesis and giving their details in the references.

(e) Whenever I have quoted written materials from other resources I have put them under the quotation marks and given due credit to them by citing them and giving their details in the references.

Thatha Divya

ACKNOWLEDGEMENTS

It is my immense pleasure to avail this opportunity to express my gratitude, regards and heartfelt respect to Prof. Susmita Das, Department of Electrical Engineering, NIT Rourkela for her endless and valuable guidance prior to, during and beyond the tenure of the project work. Her priceless advices have always lighted up my path whenever I have struck a dead end in my work. It has been a rewarding experience working under her supervision as she has always delivered the correct proportion of appreciation and criticism to help me excel in my field of research.

I would like to express my gratitude and respect to Prof. K. R. Subhashini, Prof. D. Patra, Prof. P. K. Sahu and Prof. S. Gupta for their support, feedback and guidance throughout my M. Tech course duration. I would also like to thank all the faculty and staff of EE department, NITR for their support and help during the two years of my student life.

I would like to make a special mention of the selfless support and guidance I received from my seniors Kiran Kumar Gurrala, Deepak Kumar Rout, Deepa Das, Ch.Manoj Kumar Swain and Subhankar Chakrabarti during my project work. Also I would like to thank Rati Jalan, Pruthvi Raj Kumar, and Bishnu Prasad Sahoo for making my hours of work in the laboratory enjoyable with their endless companionship and help as well.

Last but not the least; I would like to express my love, respect and gratitude to my parents, younger brother and sister, who have always supported me in every decision I have made, believed in me and my potential and without whom I would have never been able to achieve whatsoever I could have till date.

Above all, I thank Almighty who bestowed his blessings upon us.

THATHA DIVYA

ABSTRACT:

In present communication scenario, security and privacy of data being transmitted is very difficult due to the broadcast nature of wireless medium. To secure and protect the confidentiality of data being transmitted, physical layer security offers attractive solutions using cooperative relaying schemes, in which relay assists the transmission of data between source and destination.

In this work, we consider a cooperative wireless network in which relay either tries to improve the channel capacity of source to destination link using cooperative relaying protocols or reduce the channel capacity of source to eavesdropper link using jamming techniques. In order to improve the performance of the communication system, optimal relay and jammer are selected based on the three proposed relay and jamming selection schemes namely Conventional selection (Without jamming), Optimal selection with jamming (OSJ) and Optimal selection with control jamming (OSCJ).

Optimal relay forwards the source information using cooperating relaying protocols such as decode and forward(DF), Amplify and Forward(AF) ,Hybrid decode amplify forward (HDAF) which combines the benefits of both DF and AF schemes. At the same time, jammer generates artificial noise using cooperative jamming scheme, to confuse the eavesdropper. The received signals at the receiver are combined using the various diversity techniques such as maximum ratio combining (MRC) and fixed ratio combining (FRC) techniques.

Monte Carlo simulations are carried out and the obtained results are compared for different relay, jammer and eavesdropper locations. A study of comparison is made in terms of secrecy capacity and intercept probability for the proposed relaying schemes in the presence of single eavesdropper. Finally from the simulated comparison study, it is observed that HDAF scheme outperforms AF and DF schemes and we can also observe control jamming selection achieves more secrecy rate compared to without jamming and with optimal jamming.

Contents

ABBREVIATIONS

DF	:	Decode and Forward
AF	:	Amplify and Forward
CJ	:	Cooperative Jamming
HDAF	:	Hybrid Decode-Amplify-Forward
MRC	:	Maximum Ratio Combining
SC	:	Selection Combining
EGC	:	Equal Gain Combining
SNRC	:	Signal to Noise Ratio Combining
CSI	:	Channel Static Information
AWGN	:	Additive White Gaussian Noise
SNR	:	Signal to Noise Ratio
MER	:	Main to Eavesdropper Ratio
TDMA	:	Time Division Multiple Access
QPSK	:	Quadrature Phase Shift Keying
CS	:	Conventional Selection
OSJ	:	Optimal Selection with Jamming
OSCJ	:	Optimal Selection with Control Jamming

LIST OF FIGURES:

LIST OF Tables:

1

INTRODUCTION

1.1 Overview

Recent days, security plays an important role in communication systems as more number of people depends on wireless network, to transmit their personal data. But the openness of the wireless medium makes it very difficult, as unauthorised users can overhear the transmission. To protect the confidentiality of data, physical layer security provides the best solution, by exploiting the physical layer properties of the wireless medium.

Initially Cryptographic protocols are used for the improvement of security at application layer. But they are highly complex and detection of private key became easier for the attackers. Physical layer security (PLS) can be used to improve the security of wireless network without any encryption or decryption techniques. To improve the channel quality of legitimate receiver's link, physical layer security exploits the characteristics of channel or the transmission medium.

Traditional physical layer security techniques are based on single antenna systems. These systems offer several drawbacks. If the channel capacity of source-legitimate receiver link is less than the channel capacity of source-illegitimate receiver link, then the secrecy rate becomes typically zero. And also the channel characteristics are affected by the absence of feedback. To overcome the limitations of single antenna systems, multiple antenna systems are introduced namely Single Input Multiple Output, Multiple Input Multiple Output etc... But because of high cost and size, implementing multiple antennas at each and every node becomes difficult. In this situation, node cooperation offers attractive solution by enabling the systems with single antenna users to get the advantages of multiple antennas.

In node cooperation, optimal relay uses cooperating relaying schemes, decode and Forward, Amplify and Forward, Hybrid Decode-Amplify-Forward to transmits the source information to legitimate receiver, meanwhile jammer generates artificial noise to confuse the eavesdropper.

In this thesis we considered two performance parameters named as Secrecy capacity and intercept probability. Secrecy capacity is termed as maximum secrecy rate which is defined as the difference between the channel capacities of transmitter-legitimate receiver link and transmitter-illegitimate receiver link. Intercept probability is defined as the probability of occurrence of an intercept event which will happen when secrecy capacity falls below zero.

Among all the cooperating relaying schemes, HDAF relaying produces best results by employing, DF scheme until relay decodes the message perfectly and AF scheme if relay cannot be able to decode the message.

1.2 Literature Survey

Recently cooperative communication attained many people attention because of openness of wireless medium which causes the eavesdroppers to overhear source information. The main idea of cooperative communication is to transmit the signal from transmitter to legitimate receiver, with the help of friendly neighbouring nodes called as relays.

Wireless systems are experiencing severe fading due to the multipath propagation of signal. To combat fading effects, diversity techniques are developed. Diversity techniques allow each user to have multiple antennas, for transmitting the signal but due to the cost and size limitation, many networks are limited to single antenna nodes **[1]**. Cooperative communication uses spatial diversity which allows single antenna users to gets the benefits of multiple antennas by sharing their antennas with the neighbouring nodes.

Authors in **[1]** explained a brief description about the wireless cooperative networks and the signalling schemes to transmit the signals. Amplify and Forward and Decode and Forward are the two elemental relaying schemes used by the relays, to transmit the signal to destination.

In AF cooperative relaying, relay first amplifies the arrived transmitter signal and transmits to legitimate receiver. To mitigate the effect of eavesdropper on the source signals authors in **[5]** explained about AF relaying, in the presence single and multiple eavesdroppers. They have provided optimal solutions for single eavesdropper and sub optimal solutions for multiple eavesdroppers to improve the performance of wireless cooperative network.

In DF cooperative relaying, relay decodes the arrived information signal, re-encode it and transmits to destination. Authors in **[7]** proposed two relaying schemes using DF named as Cooperative MRC scheme and Alamouti scheme and they proved that Alamouti scheme performs better when phase synchronization is not available and cooperative MRC scheme performs better when phase synchronization is available.

A comparative study of AF and DF relaying schemes was proposed in **[9-10]**. **[9]** and **[10]** papers showed the comparison in terms of error probability and proved both relaying schemes are not much different and slightly DF performs better than AF relaying. In order to improve the performance of cooperative wireless network, optimal relay selection is proposed in **[11]** and it showed the comparison study of Traditional MRC techniques and practical optimal relay selection for both AF and DF relaying schemes in terms of intercept probability and diversity order. In the case of diversity order both the schemes achieved the same diversity order M where M is number of relays. Results showed that optimal relay selection performance much better in terms of intercept probability than traditional MRC scheme.

In order to reduce the channel capacity of source to eavesdropper link, a new technique cooperative jamming is proposed. In Cooperative jamming (CJ), while source transmitting the information signal, relay transmits jamming signals to confuse the eavesdropper. **[14]** paper explained about the three cooperative schemes DF, AF and CJ in the presence of single and multiple illegitimate receivers and proposed two practical design problems i.e. maximizing the secrecy rate considering transmitting power as a constraint and minimizing the transmit power considering the secrecy rate as a constraint.

An approach of source and relay uses some of their power to transmit the artificial noise signal to eavesdropper is investigated in **[23]**. A special case, where relay assisted the eavesdropper using AF, DF and CF (Compress and Forward) techniques and also the effect of path loss on secrecy rate were analysed in **[20]**. Based on the knowledge of the eavesdropper channel, a new relay and jammer selection schemes are proposed in **[21]**. Effect of relay location on Bit Error rate (BER) is analysed and application of genetic algorithm to find out the optimal relay location is explained in **[22]**. The ergodic secrecy rate is derived by calculating the Moment generating function (MGF) of SNR's is explained in **[23]**.

A new adaptive hybrid relaying scheme is proposed in **[26]**, which switches between AF and adaptive DF based on the decoding capability of the relay. A hybrid relaying scheme which switches between AF and adaptive DF for multiple relays was proposed and the performance was analysed in **[27]**. SNR based hybrid relaying for single relay was proposed and performance was analysed in **[29]**.

In this thesis, SNR based multiple HDAF relay cooperative network is considered and the performance was analysed for the proposed relay and jamming selection schemes, namely conventional selection (Without jammer), optimal selection (With jammer) and control jamming. Secrecy capacity which is the difference between the channel capacity of main and eavesdropper links was analysed for each relay and jammer selection and it was also analysed for different path loss indices.

1.3 Motivation

Privacy of data being transmitted has taken considerable attention due to the openness of wireless network which allows the eavesdroppers to overhear the source information. Earlier cryptographic protocols increase the potential attackers because of easier key detection. Physical layer security overcomes these limitations and provides better solution by employing cooperative relaying schemes. The problem here is, to improve the secrecy rate even when the channel capacity of source-illegitimate receiver link is more than the source-legitimate receiver link with help of cooperative relaying and hamming schemes.

1.4 Objectives

The main objectives of the thesis work are:

1. To study the importance of jamming performance in cooperative communication
2. To study various relay and jammer selection schemes such as conventional jamming (CS), optimal selection with jamming (OSJ) and optimal selection with control jamming (OSCJ).
3. To study various cooperative relaying protocols such as Decode and Forward (DF), Amplify and Forward (AF), Cooperative jamming (CJ) and Hybrid Decode-Amplify-Forward (HDAF).
4. To calculate the secrecy capacity of DF, AF, CJ and HDAF relaying schemes.
5. To calculate the intercept probability of AF cooperative relaying scheme with single and multiple relays.
6. To explore the effect of relay and eavesdropper positions on secrecy capacity.
7. To evaluate the path loss effect on the performance of system.

1.5 Thesis Contribution

The ultimate aim of the cooperative communication is to transmit the signal to the destination perfectly and providing privacy against the attacks of eavesdropper or illegitimate receiver.

The contribution of the thesis includes the following points:

- Improving the Secrecy rate by employing HDAF cooperative relaying scheme.
- Providing better privacy using control jamming scheme.
- Finding the optimal location of the relay and jammer to improve the performance of the cooperative wireless network

1.6 Thesis Organisation

The thesis has been organised into 6 chapters.

Chapter 1: This chapter explains the overview of the cooperative communication, motivation to take up this research work, objectives and literature survey. This chapter gives the brief introduction of the cooperative communication.

Chapter 2: This chapter gives the brief introduction of cooperative wireless network, phases of signal transmission, simplified cooperation model. It also explains about the various cooperative relaying schemes such as DF, AF and HDAF.

Chapter 3: This chapter discusses about the importance of jamming in wireless communication and various relay and jammer selection schemes such as CS, OSJ and OSCJ to improve the secrecy rate against attacks of eavesdropper.

Chapter 4: This chapter explains about the various diversity combining techniques at the receiver node such as ERC, MRC, SNRC and SC to combine the multiple copies of the transmitted information.

Chapter 5: This chapter discusses about performance analysis of cooperative relaying schemes in the presence of single illegitimate receiver. It also gives the mathematical analysis of secrecy capacity and intercept probability of the cooperative relaying schemes for single and multiple relays. The simulation results have been included to validate the theoretical analysis.

Chapter 6: This chapter explains the conclusion of the entire research work discussed and scope of further possibilities of this work.

2

BACKGROUND STUDY ON COOPERATIVE WIRELESS NETWORK

2.1 Introduction

In Cooperative communication, introduction of relay channel generates few more independent paths between source and destination along with the direct link. The total communication process occurs in two stages namely broadcasting stage and cooperating stage.

- In broadcasting stage, Source sends its information to destination via a transmission medium. But due to openness of wireless network, relay and eavesdropper overhears the source information.
- In cooperating stage, Relay processes the received source signal, using one of the cooperating relaying schemes and it sends the processed signal to its legitimate receiver. At the same time jammer generates the artificial noise to reduce the channel capacity of source to eavesdropper link.

The main aspect of this cooperative communication is processing of the received source signal done by the relay. These different processing schemes at relay, leads to different cooperative relaying protocols.
Cooperative communication schemes are generally categorized into two types:

1. Fixed relaying scheme.
2. Adaptive relaying scheme.

In Fixed relaying scheme, all the resources of channel are shared between source and relay in a fixed manner. Processing at the relay differs for each protocol. In fixed amplify and forward (AF) relaying, relay simply forwards the received source signal to destination where as in fixed decode and forward (DF) relaying, relay decodes the arrived information signal, re-encode it and sends to legitimate receiver. Implementation of fixed relaying schemes is easier but the efficiency of bandwidth is low because of

sharing, half of resources of channel to relay. If the source-legitimate receiver link is more, sharing half of resources to relay becomes useless since the source can send its information signal to destination directly.

To overcome the limitations of fixed relaying, Adaptive relaying comp selective and incremental relaying. In selective relaying, if the SNR of the arrived signal at the helper exceeds a certain margin value it implements one of the cooperative relaying protocols and sends the processed information signal to destination. If SNR of the arrived signal at relay is less than the margin, it will be in idle position. In incremental relaying, if destination not able to decode the message, source resends the information signal via relay.

2.1.1 Advantages of Cooperative Communication:

Cooperative communication has several benefits in wireless networks such as:

- Lower interference
- High diversity gain
- Higher throughput and lower delay.

2.1.2 Applications of Cooperative Communication:

Some of the applications of cooperative communication include:

- Virtual antenna array
- Ad-hoc networks
- Military applications
- Cognitive radio
- Wireless sensor networks like patient monitoring systems.

2.1.3 Simplified cooperation model

In this unit, a simple cooperative wireless network with helper in the presence of single eavesdropper is shown in the figure. Total communication process occurs in two stages. First phase is called broadcasting stage, in which source broadcasts its information to legitimate receiver with power P_s, but because of broadcast nature of transmission medium relay and eavesdropper overhears the source information.
Arrived signals at the destination, relay and eavesdropper are given as below [11]:

$$Y_{s,d} = \sqrt{P_s} H_{s,d}^{*} S + n_d \qquad [1]$$

$$Y_{s,r} = \sqrt{P_s} H_{s,r}^{*} S + n_r \qquad [2]$$

$$Y_{s,e} = \sqrt{P_s} H_{s,e}^{*} S + n_e \qquad [3]$$

Here P_s is transmitted power by the source node with which information signal can be transmitted, S is transmitted message from source, $H_{s,d}$ is the channel coefficient of transmitter and legitimate receiver link, $H_{s,r}$ is the channel coefficient of source-helper link, $H_{s,e}$ is the channel coefficient of the transmitter and illegitimate receiver and the noise terms n_d, n_r, n_e are additive white Gaussian noises with zero mean and variance as one, at destination, relay and eavesdropper respectively.

Second stage is called as cooperating stage, in which relay processes the received information signal using one of the cooperating relaying protocol and sends the processed signal with power P_r, to its intended receiver. At the same time one of the relay selected as a jammer, to produce artificial interference with power P_j, to confound the eavesdropper.

Arrived signals at the legitimate receiver, eavesdropper given as below [15]:

$$Y_{r,d} = \sqrt{P_r} H_{r,d}^{*} \tilde{S} + \sqrt{P_j} H_{j,d}^{*} Z + n_d \qquad [4]$$

$$Y_{r,e} = \sqrt{P_r} H_{r,e}^{*} \tilde{S} + \sqrt{P_j} H_{j,e}^{*} Z + n_e \qquad [5]$$

Here P_r is the power transmitted by the relay node, $H_{r,d}$ is the rayleigh channel coefficient of helper-destination link, $H_{r,e}$ is the rayleigh channel coefficient of helper node and eavesdropper link, $\tilde{S}$ is the processed information signal according to the selected cooperative relaying scheme, P_j is the transmitted power of jammer with which artificial noise can be transmitted and is equal to P_r/L (To protect destination from the jamming signal).Where L denotes the ratio of relay power to jammer power and is greater than 1, Z is the artificial noise signal generated at jammer , $H_{j,d}$ is the rayleigh channel fading coefficient of jammer and destination link ,$H_{j,e}$ is the rayleigh channel fading coefficient of jammer and eavesdropper link and n_d, n_e are the AWGN noises with zero mean and variance 1 at destination and eavesdropper respectively.

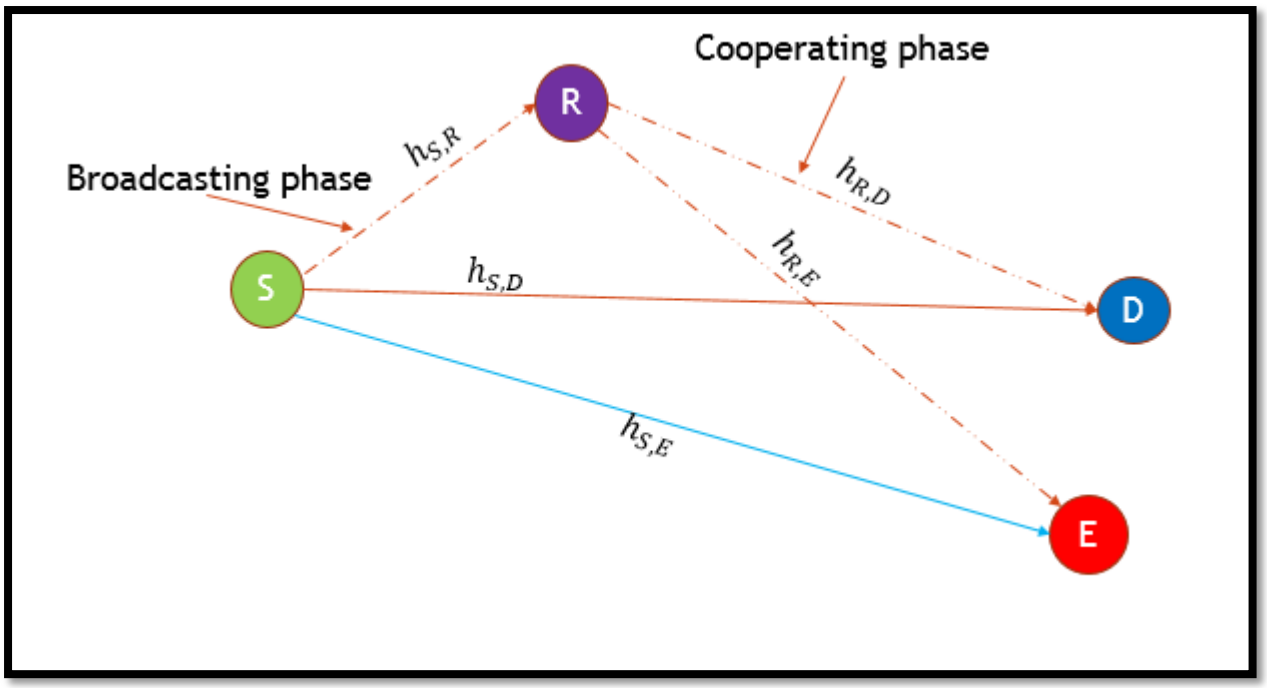

Fig 2.1: Simplified Cooperative Model

2.2 Cooperating Relaying Schemes:

After receiving the information signal from the source, relay uses cooperating relaying schemes to process the signal. Elemental cooperating relaying schemes to transmit the information signal to the destination are Decode and Forward (DF) and Amplify and Forward (AF). In addition to these two relaying schemes, Cooperative jamming is used by the relay, to produce artificial interference to confound the eavesdropper. To combine the benefits of both DF and AF, a new cooperating relaying scheme Hybrid Decode-Amplify-Forward (HDAF) is introduced in this chapter.

2.2.1 Decode and Forward (DF):

In decode and Forward (DF) relaying scheme, relay first decodes the received source signal, then re-encode it and forwards to the destination. When the signal to noise ratio of the received source signal exceeds a certain threshold value, relay can perfectly decode the signal. Arrived signals at the destination and eavesdropper are given as [11]:

$$Y_{r,d} = \sqrt{P_r} H_{r,d}^{*} S_{DF} + n_d \qquad [6]$$

$$Y_{r,e} = \sqrt{P_r} H_{r,e}^{*} S_{DF} + n_e \qquad [7]$$

Here P_r is the power transmitted by the relay node, $H_{r,d}$ is the rayleigh channel fading coefficient of helper-destination link, $H_{r,e}$ is the rayleigh channel fading coefficient of helper-eavesdropper link, S_{DF} is the processed information signal using decode and Forward (DF) cooperative relaying scheme and n_d, n_e are the AWGN noises with zero mean and variance 1 at destination and eavesdropper respectively.

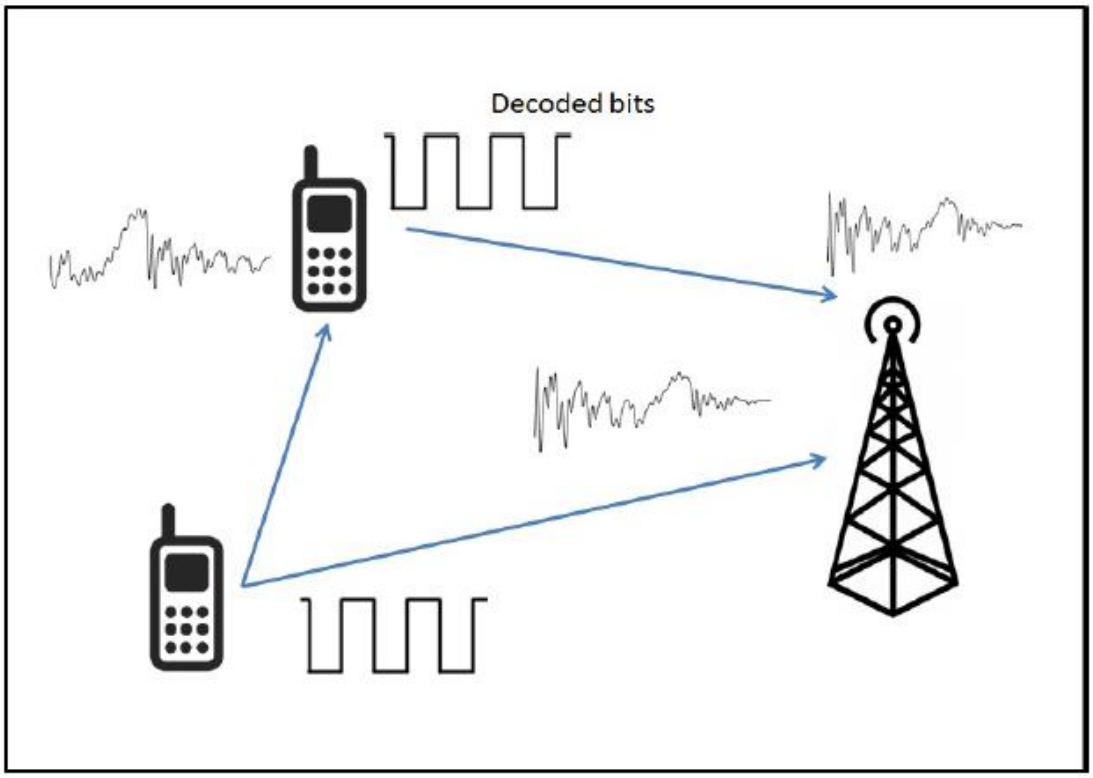

Fig 2.2: Decode and Forward (DF) Relaying Scheme

2.2.2 Amplify and Forward (AF):

In Amplify and Forward (AF) relaying protocol, relay first amplifies the received information signal and then forwards to the destination. But the disadvantage with AF relaying is, it also amplifies the noise signal along with the information signal. Arrived signals at the destination and eavesdropper are given as [11]:

$$Y_{r,d} = \sqrt{P_r} H_{r,d}^{*} S_{AF} + n_d \qquad [8]$$

$$Y_{r,e} = \sqrt{P_r} H_{r,e}^{*} S_{AF} + n_e \qquad [9]$$

Here $S_{AF} = \left(\frac{Y_{s,r} H_{s,r}^{*}}{\sqrt{P_r} |H_{s,r}|^2} \right)$ is the amplified signal,

P_r is the power transmitted by the relay node, $H_{r,d}$ is the rayleigh channel fading coefficient of helper-destination link, $H_{r,e}$ is the rayleigh channel fading coefficient of helper-eavesdropper, S_{DF} is the re-encoded signal at the best relay and n_d, n_e are the AWGN noises with zero mean and variance as 1 at destination and eavesdropper respectively

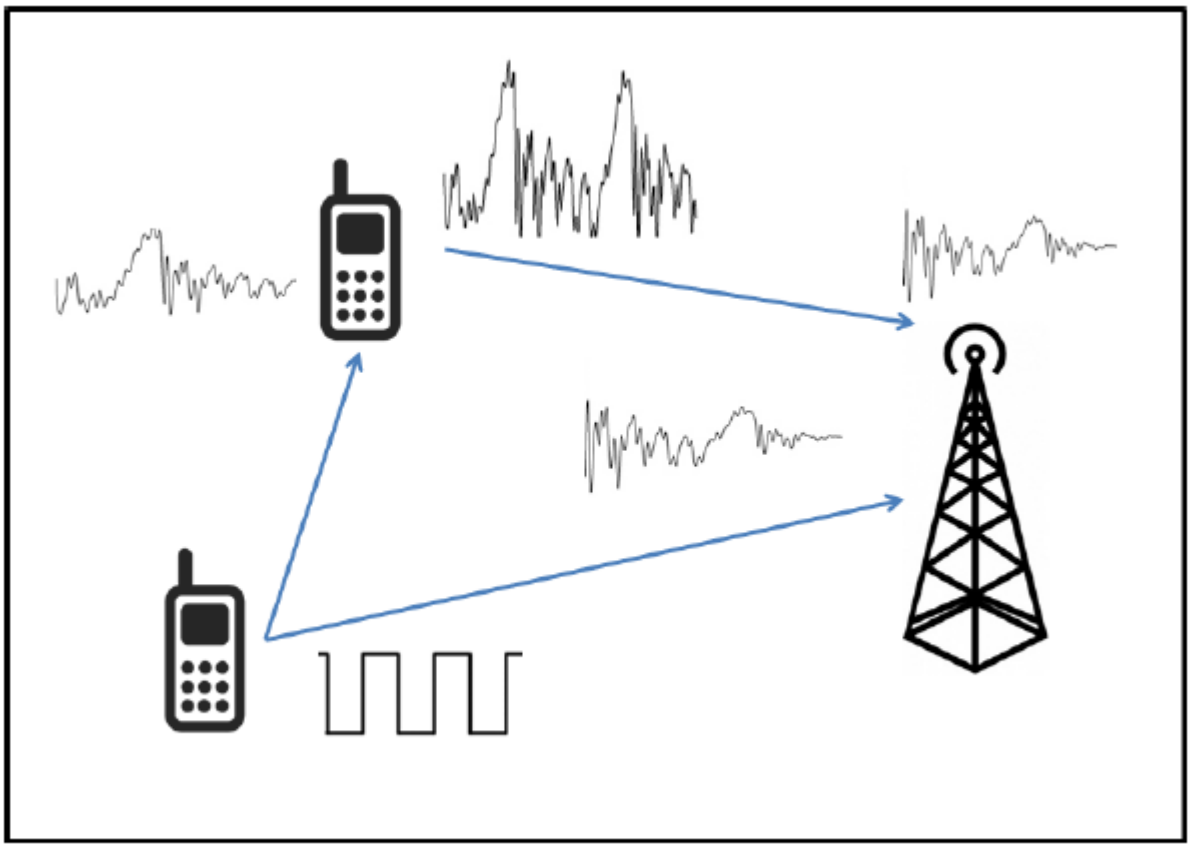

Fig 2.3: Amplify and Forward Relaying Scheme

2.2.3 Cooperative Jamming (CJ):

When illegitimate receiver channel is more than the legitimate receiver channel, secrecy capacity becomes zero. To avoid this problem, cooperating jamming is introduced to create intentional interference at the illegitimate receiver with the help of jammer.

In Cooperative Jamming (CJ), when the source is transmitting the information signal, at the same time one of the relay selected as a jammer to produce artificial noise, to confound the illegitimate receiver. Arrived signals at the destination and eavesdropper are given as [15]:

$$Y_{r,d} = \sqrt{P_r} H_{r,d}^{*} \tilde{S} + \sqrt{P_j} H_{j,d}^{*} Z + n_d \qquad [10]$$

$$Y_{r,e} = \sqrt{P_r} H_{r,e}^{*} \tilde{S} + \sqrt{P_j} H_{j,e}^{*} Z + n_e \qquad [11]$$

Here P_r is the transmitted power of relay node, $H_{r,d}$ is the rayleigh channel coefficient between the relay and destination, $H_{r,e}$ is the rayleigh channel coefficient of helper- eavesdropper, $\tilde{S}$ is the processed information signal according to the selected cooperative relaying scheme, P_j is the transmitted power of jammer with which artificial noise can be transmitted and is equal to P_r/L (To protect destination from the jamming signal).Where L denotes the ratio of relay power to

jammer power and is greater than 1, Z is the artificial noise signal generated at jammer , $H_{j,d}$ is the rayleigh channel fading coefficient of jammer- destination link,$H_{j,e}$ is the rayleigh channel fading coefficient of jammer-eavesdropper link and n_d, n_e are the AWGN noises with zero mean and variance 1 at destination and eavesdropper respectively.

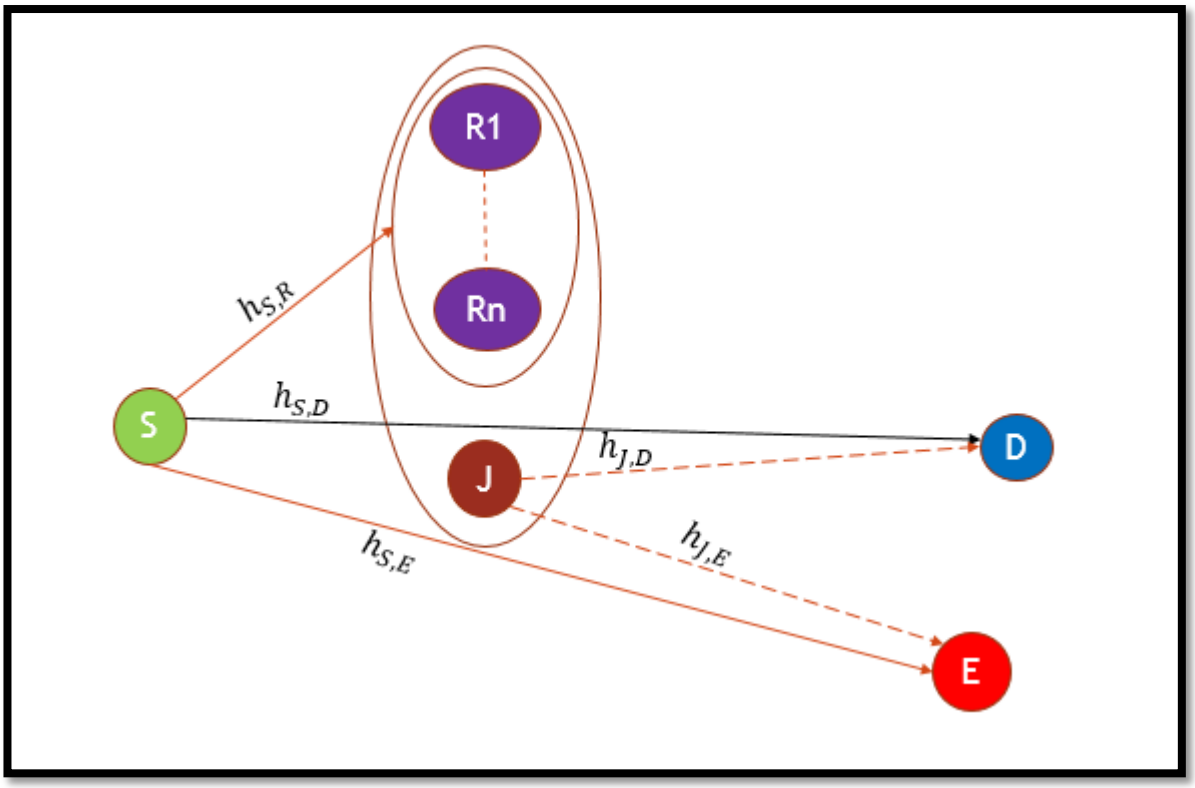

Fig 2.4: Cooperative Jamming (CJ)

2.2.4 Hybrid Decode Amplify Forward (HDAF) Relaying:

In decode and forward relaying, relay can decode the signal impeccably if it near is to the destination and when relay is far away from source, amplify and forward relaying can gives the better result compared to decode and forward. A new hybrid relaying scheme Hybrid Decode Amplify Forward (HDAF) is proposed in order to get the benefits of both DF and AF relaying schemes.

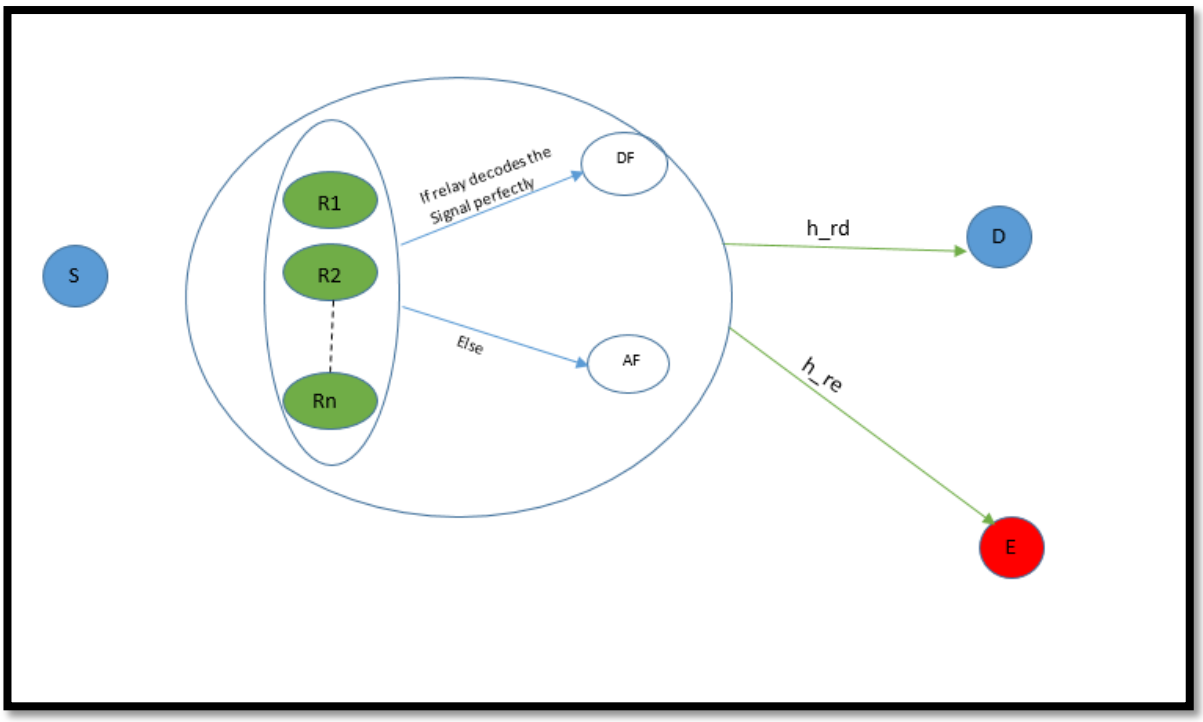

Fig 2.5: Hybrid Decode-Amplify-Forward (HDAF) Relaying Scheme

HDAF	=	DF	If relay can decode the signal impeccably
	=	AF	else

2.3 Summary

In this chapter we considered a wireless network in which all the relays participate in cooperating phase. In order to improve the performance of the wireless network against the malicious eavesdropper attacks, optimal relay need to be selected for transmitting the information signal to the destination and the remaining relays should act as jammers to confound the eavesdropper. So next chapter deals with the relay and jammer selection schemes in order to improve performance of the system.

3

SECURITY IN COOPERATIVE WIRELESS NETWORK

3.1 Introduction:

In order to provide the security to the data being transmitted against eavesdropper attacks, an optimal relay and jammer needs to be selected. In second phase of transmission called as cooperating phase, the relay which is having the highest signal to noise ratio needs to be selected as an optimal relay and the relay which is having low signal to noise ratio needs to be selected as a jammer, so that different relays can be used in cooperating and jamming.

3.2 Relay and Jammer Selection Methods:

The effect of jamming can be well understood by considering three different relay and jammer selection schemes which are explained in detail in the next subsections.

3.2.1 Conventional Selection (Without Jamming):

This selection does not involve any jamming process, hence in cooperative phase only the relay which is having high signal to noise ratio is selected to accesses the channel and sends information to the destination. This selection assumes that the source-eavesdropper links and relay-eavesdropper links are not available. It selects the best relay based on the instantaneous SNR values of helper-destination channel link and source-destination channel link and is expressed as [21]:

$$R^* = max_{R \in C_d}(1 + SNR_{sd} + SNR_{rd}) \quad [12]$$

Where R belongs to the decoding set $C_d \subset S_{relay}$

Secrecy capacity for conventional selection is expressed as [21]:

$$C_S^{|C_d|}(R) = \max\left(0, 0.5\, log_2\left(\frac{1 + SNR_{sd} + SNR_{rd}}{1 + SNR_{se} + SNR_{re}}\right)\right) \quad [13]$$

where $\mathrm{SNR_{rd}}$ is the SNR of helper-destination channel link, $\mathrm{SNR_{re}}$ is the SNR of helper-eavesdropper channel link, $\mathrm{SNR_{sd}}$ is the SNR of transmitter-legitimate receiver channel link, $\mathrm{SNR_{se}}$ is the SNR of transmitter-illegitimate receiver channel link.

3.2.2 Optimal Selection with Jamming (OSJ):

This selection process involves jamming process. While selecting the cooperative relay and jammer, it assumes that relay-eavesdropper links are available and it also assumes that the destination is unaware of the jamming nodes. In OSJ, cooperative relay and jammer nodes are selected based on the equations given as [21]:

$$R^* = \max_{R \in C_d}\left(\frac{SNR_{rd}}{SNR_{re}}\right) \quad [14]$$

$$J^* = \max_{J \in S_{relay}}\left(\frac{SNR_{je}}{SNR_{jd}}\right) \quad [15]$$

where R* is optimal relay and J* is jammer

In this, relay selection tries to improve the ratio of, SNR_{rd} and SNR_{re} and the jammer selection tries to improve the ratio of, SNR_{je} and SNR_{jd}.Hence, we can select different relays for cooperation and jamming.

The secrecy capacity for OSJ method is expressed as [21]:

$$C_S^{|C_d|}(R, J) = \max\left(0, 0.5\, log_2\left(\frac{1 + \frac{SNR_{sd}}{1 + SNR_{jd}} + \frac{SNR_{rd}}{1 + SNR_{jd}}}{1 + \frac{SNR_{se}}{1 + SNR_{je}} + \frac{SNR_{re}}{1 + SNR_{je}}}\right)\right) \quad [16]$$

where SNR_{rd} is the SNR of helper-destination channel link, SNR_{jd} is the SNR of jammer-destination channel link,SNR_{je} is the SNR of jammer-eavesdropper channel link, SNR_{re} is the SNR of helper-eavesdropper channel link, SNR_{sd} is the SNR of transmitter-legitimate receiver channel link, SNR_{se} is the SNR of transmitter-illegitimate receiver channel link.

3.3 Optimal Selection with Control Jamming (OSCJ):

This selection scheme is proposed on the basis of assumption that the destination knows about the jamming nodes and the eavesdropper is unaware of it. Hence, only destination can decode the jamming signal, but not eavesdropper. Hence while selecting the jammer node, this selection considers only jammer to eavesdropper SNR value. In OSCJ, cooperative relay and jammer are selected based on the following equations [21]:

$$R^* = \underset{R \in C_d}{max} \left(\frac{SNR_{rd}}{SNR_{re}} \right) \quad [17]$$

$$J^* = \underset{J \in S_{relay}}{max} \left(SNR_{je} \right) \quad [18]$$

where R* is optimal relay and J* is jammer

The secrecy rate for OSCJ method can be expressed as [21]:

$$C_S^{|C_d|}(R,J) = \max\left(0, 0.5\, log_2 \left(\frac{1 + SNR_{sd} + SNR_{rd}}{1 + \frac{SNR_{se}}{1 + SNR_{je}} + \frac{SNR_{re}}{1 + SNR_{je}}} \right) \right) \quad [19]$$

where SNR_{rd} is the SNR of helper-destination channel link, SNR_{jd} is the SNR of jammer-destination channel link,SNR_{je} is the SNR of jammer-eavesdropper channel link, SNR_{re} is the SNR of helper-eavesdropper channel link, SNR_{sd} is the SNR of transmitter-legitimate receiver channel link, SNR_{se} is the SNR of transmitter-illegitimate receiver channel link.

3.4 Summary

In this chapter we have discussed the various relay and jammer selection schemes to improve the performance of the cooperative wireless network. Among all the selection schemes, optimal selection with control jamming achieves more secrecy rate and simulative study of these selection schemes are explained in chapter 5. Second and third chapter deals with the relaying schemes and selection schemes which is

performed at relay node. Now fourth chapter deals with the combining techniques of all the transmitted signal at the receiver node.

4

DIVERSITY COMBINING TECHNIQUES AT THE RECEIVER NODE

4.1 Introduction

Wireless channel undergoing severe fading due to the multi path propagation of the signal. To combat this fading, diversity techniques are developed. In cooperative communication, signal can be transmitted either directly or via relays to the destination such that multiple copies of the original signal can be received at the receiver. At the receiver node, multiple copies of the signal combined using diversity combining techniques, to get the strong signal.

In this chapter we will be discussing four important diversity combining techniques such as:

- Equal Gain combining (EGC)
- Maximal Ratio combining (MRC)
- Signal to Noise Ratio Combining (SNRC)
- Selection Combining (SC)

4.2 Equal Gain Combining (EGC)

In this technique, all the arrived signals are added together with equal gain, to get the strong signal. In cooperative communication for single relay case, we have two signals, one is the direct signal from the source and another one is processed signal from the relay.

Each received signal is multiplied by the $e^{-j\theta}$component and then added together to get the strong signal at the legitimate receiver node. The arrived signal at the legitimate receiver is given as [24]:

$$Y_d = Y_{s,d}e^{-j\theta} + Y_{r,d}e^{-j\theta}$$

[20]

where Y_d is the signal received by the destination, after applying equal gain combining technique,

$Y_{s,d}$ is the direct transmitted signal from source to destination and

$Y_{r,d}$ is the signal transmitted from relay to destination.

4.3 Maximum Ratio Combining (MRC)

In this technique, all the received signals are weighted together to get the maximum SNR at the receiver node. The following figure indicates how this technique combines the received signals.

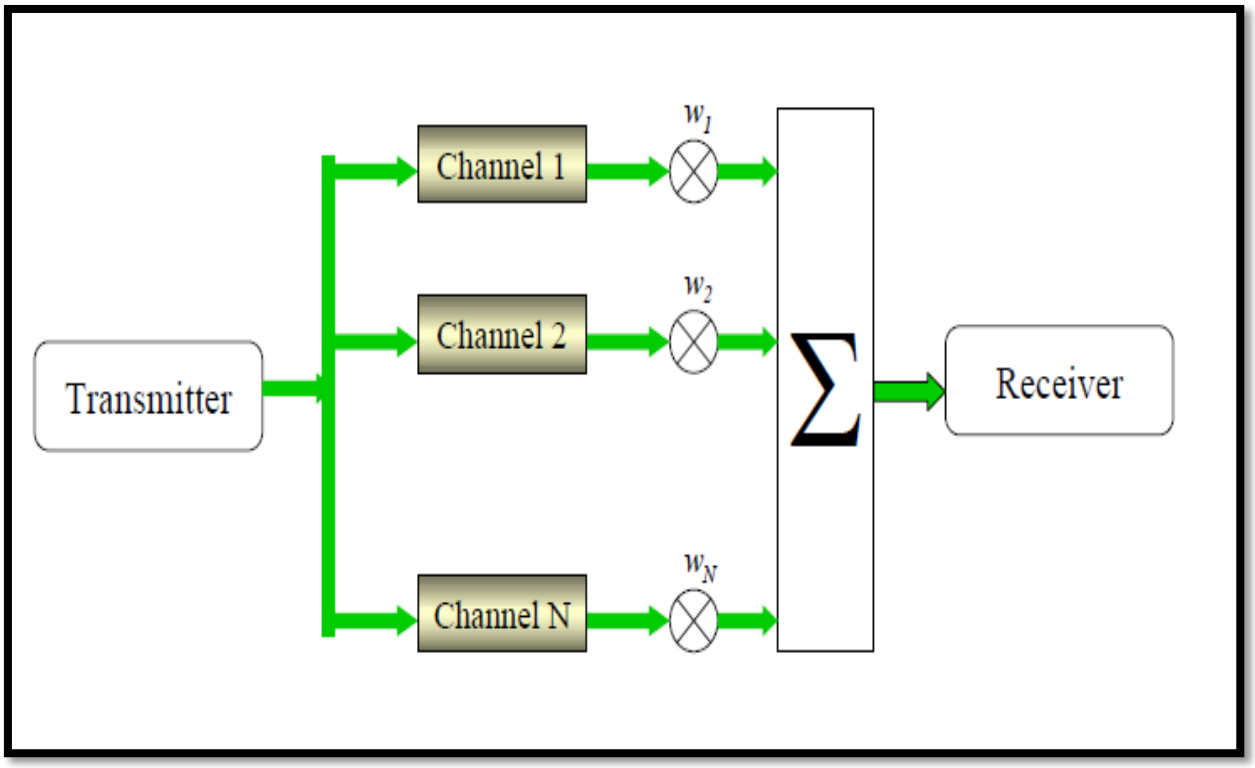

Fig 4.1: Maximum Ratio Combining

For single relay case, we have two channels one is source to destination channel, through which the direct signal can be transmitted from source to destination and another channel is relay to destination channel through which the processed signal can be transmitted from relay to destination. Weights can chose as complex conjugate of the channel gain.

The received signal at the destination after applying MRC technique for single relay case is given as [11]:

$$Y_d = Y_{s,d} H_{s,d}^* + Y_{r,d}\, H_{r,d}^* \qquad [21]$$

where Y_d is the signal received by the destination, after applying MRC technique,

$Y_{s,d}$ is the direct transmitted from transmitter to legitimate receiver,

$Y_{r,d}$ is the signal transmitted from helper to legitimate receiver,

$H_{s,d}$ is the channel coefficient of the transmitter to legitimate receiver channel and

$H_{r,d}$ is the channel coefficient of the helper to destination channel.

4.4 Signal to Noise Ratio Combining (SNRC)

This technique intelligently combines the received signal by using signal to noise ratio as a weighted parameter. The received signal at the destination after applying SNRC technique for single relay case is given as [11]:

$$Y_d = Y_{s,d} SNR_{s,d} + Y_{r,d}\, SNR_{s,r,d} \qquad [22]$$

where Y_d is the signal received by the destination, after applying SNRC technique,

$Y_{s,d}$ is the direct signal transmitted by the source to legitimate receiver,

$Y_{r,d}$ is the signal transmitted by the helper to destination,

$SNR_{s,d}$ is the SNR of the signal transmitted by the source to legitimate receiver and

$SNR_{s,r,d}$ is the SNR of the signal transmitted by the helper to destination.

4.5 Selection Combining (SC)

In this method destination selects the arrived signal which is having an high SNR. The arrived signal at the destination after applying SC for single relay case is given as:

$Y_d = Y_{s,d}$ if SNR is high for direct transmitted signal from the source

$Y_d = Y_{r,d}$ else

The following figure describes how the selection combining technique works at the receiver side.

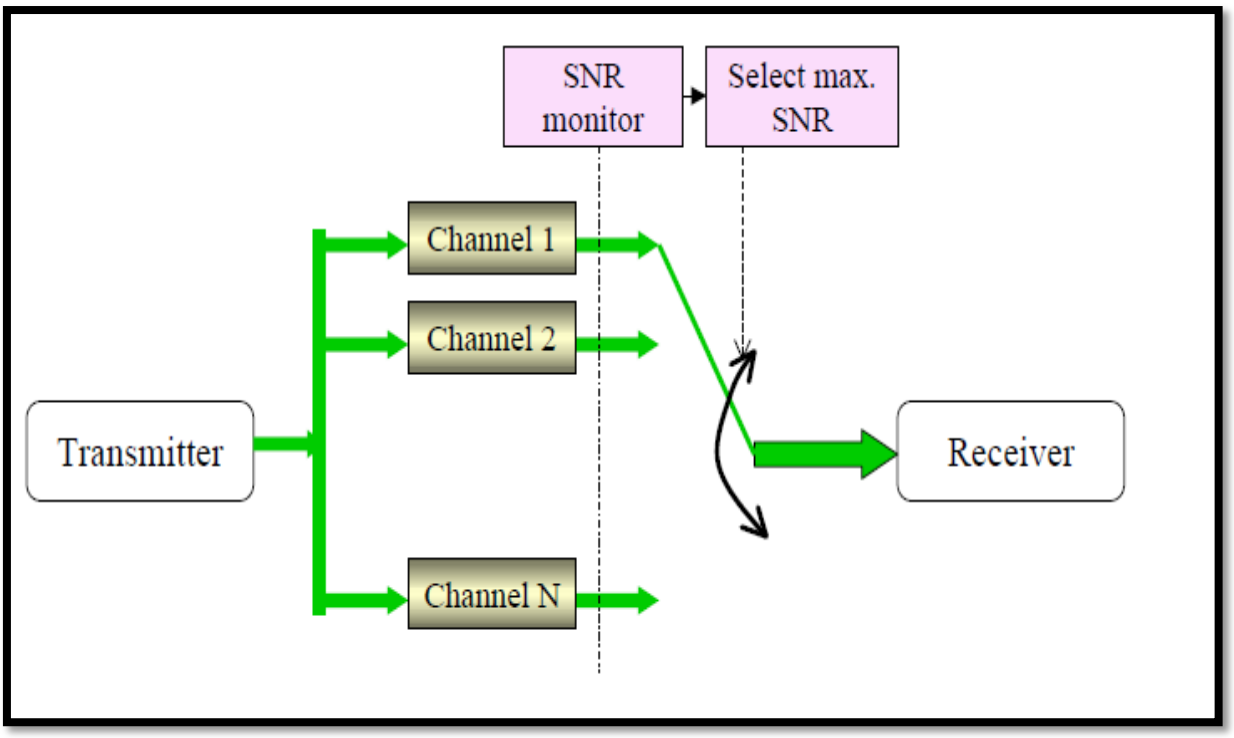

Fig 4.2: Selection Combining

4.6 Summary

This chapter discussed the various diversity combing techniques at the receiver node. Out of all the combining techniques MRC gives better performance with high complexity, EGC gives almost the equal performance of MRC and selection combining technique gives the lowest performance with low complexity. Hence for all our simulation analysis, MRC technique used as a diversity combining technique at the receiver node. Next chapter deals with the mathematical analysis of all the relaying schemes with simulative results and analysis.

5

PERFORMANCE ANALYSIS OF COOPERATIVE RELAYING SCHEMES WITH SINGLE EAVESDROPPER

5.1 System model

In this work, we consider a linear cooperative wireless network model consisting of single transmitter node (S), which sends a confidential information to the legitimate receiver node (D) with the help of half duplex mode helper nodes (R1, R2, . . . , RN) in the presence of single eavesdropper node (E). In this work all the channels undergo Flat Rayleigh fading and the authorized nodes have full channel static information (CSI) of all the communication channels. The channel gain is considered as a function of distance between two nodes and path loss index following Rayleigh fading distribution. i.e. [20]

$$h_{xy} \sim CN\left(0, {}^{1}\Big/_{d_{xy}^{\frac{c}{2}}}\right)$$

[23]

where c denotes the path loss index, varies between 2 to 4 for different environments and d_{xy} is the Euclidian distance between two nodes x and y, where x=Source, Relay, y=Relay, Destination and Eavesdropper and $x \neq y$.

It is also assumed that given network is employed by the TDMA protocol where source transmits its information during the first time slot and relays transmit information during the second time slot. The communication process from source to destination is performed in two stages named as broadcasting stage and cooperative stage as shown in Fig 5.1 and Fig 5.2.

5.1.1 Broadcasting phase:

During this stage, the source broadcasts its information with power Ps, to all the trusted relays and destination but due to the openness of the transmission, eavesdropper overhears the source information. In order to improve performance of the system, one relay node is selected to operate as a jammer in order to produce artificial noise at the eavesdropper. Arrived signals at the legitimate receiver, i^{th} relay and eavesdropper respectively are given in equation [1], [2] and [3].

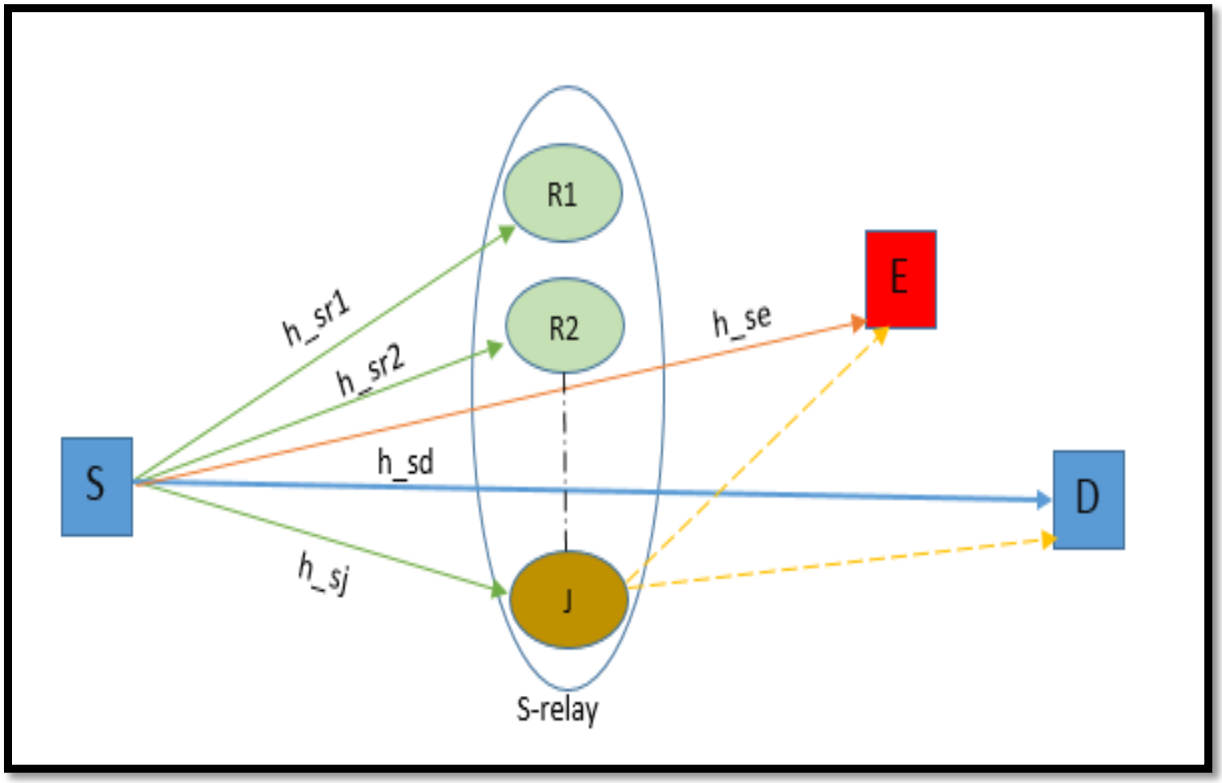

Fig 5.1: Broadcasting phase

5.1.2. Cooperating phase

During this stage, one out of N relays is selected on the basis of three proposed selection schemes, to improve the achievable secrecy rate through cooperation and one more relay is selected from the remaining N-1 relays to operate as a jammer. The cooperative relay operates in DF, AF or HDAF mode. In HDAF relaying, if the cooperative relay impeccably decodes the received information signal, then it operates in DF mode or else it operates in AF mode. When the relay operates in DF mode, then arrived signals at the legitimate receiver and illegitimate receiver are given in equation [6] and [7].

When the relay operates in AF mode, then arrived signals at the destination and eavesdropper are given in equations [8] and [9].

The second jammer is used to create artificial noise at the unauthorized node. The destination will not be able to mitigate the interference if it is unaware of the jammer nodes. Arrived signals at the legitimate receiver and the illegitimate receiver from the jammer node are given as [11]

$$Y_{jd} = \sqrt{P_j} H_{jd}^* S_j + n_d \quad [24]$$

$$Y_{je} = \sqrt{P_j} H_{je}^* S_j + n_e \quad [25]$$

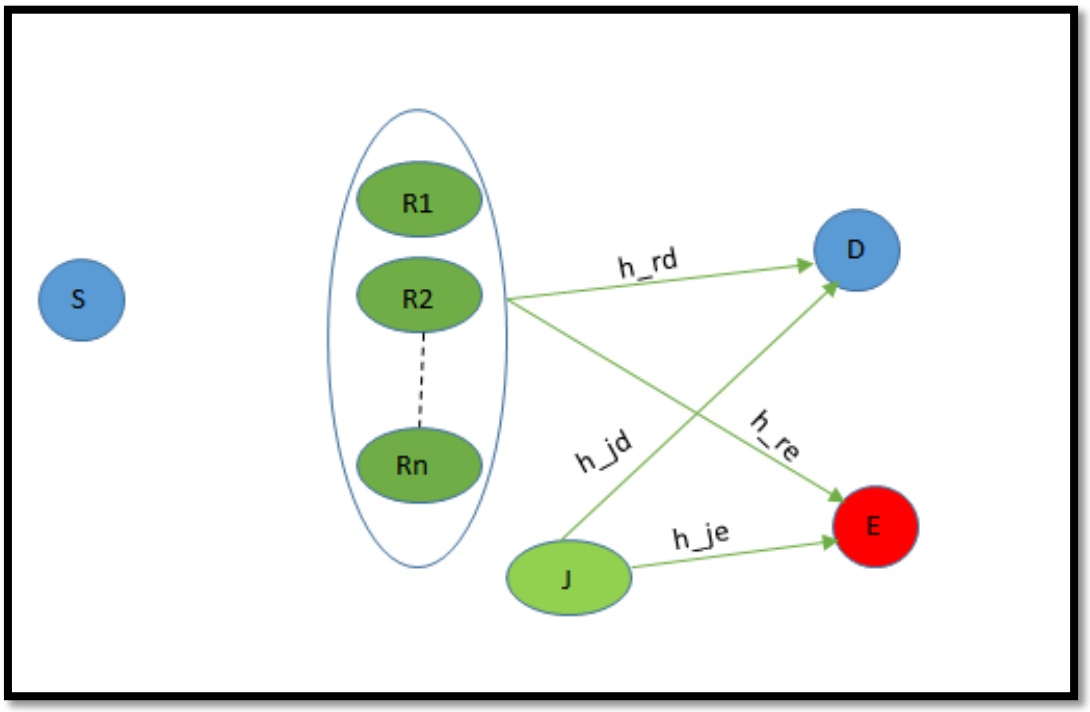

Fig 5.2: Cooperating phase

Where P_j is the transmitted power of jammer with which artificial noise can be transmitted and is equal to P_r/L (To protect destination from the jamming signal).Where L denotes the ratio of relay power to jammer power and is greater than 1, S_j is the artificial noise signal generated at jammer , H_{jd} is the rayleigh channel coefficient of jammer-destination link,H_{je} is the rayleigh channel coefficient of jammer-eavesdropper and n_d, n_r are the AWGN noises with zero mean and variance 1 at destination and eavesdropper respectively.

For comparative analysis direct transmission without relay is explained here.Consider that the source transmits its information signal to the destination with total power P. Arrived signal at the destination and eavesdropper are given as [11]:

$$Y_d = \sqrt{P} H_{s,d}^* S + n_d \quad [26]$$

$$Y_e = \sqrt{P} H_{s,e}^* S + n_e \quad [27]$$

Where P is the total transmitted power, $H_{s,d}$ is the channel coefficient of transmitter-legitimate receiver link, $H_{s,e}$ is the channel coefficient of transmitter-illegitimate receiver link, S is the information signal and n_d, n_e are the AWGN noises with zero mean and variance as 1 at destination and eavesdropper respectively.

SNR of the signal arrived at the destination is given as [8]:

$$SNR_{s,d} = \frac{P*|h_{s,d}|^2}{\sigma_d^2} \quad [28]$$

where P is the total transmitted power, $h_{s,d}$ is the channel gain of transmitter-legitimate receiver and σ_d^2 is AWGN noise variance at the destination.

SNR of the signal arrived at the eavesdropper is given as [8]:

$$SNR_{s,e} = \frac{P * |h_{s,e}|^2}{\sigma_e^2} \quad [29]$$

where P is the total transmitted power, $h_{s,e}$ is the rayleigh channel gain of transmitter to eavesdropper and σ_e^2 is AWGN noise variance at the eavesdropper.

According to Shannon's theorem the channel capacity is given as [8]:

$$C = \frac{1}{2}\log_2(1 + SNR) \quad [30]$$

The instantaneous channel capacity of source to destination is given as [8]:

$$C_{s,d} = \frac{1}{2}\log_2\left(1 + \frac{P * |h_{s,d}|^2}{\sigma_d^2}\right) \quad [31]$$

The instantaneous channel capacity of source to eavesdropper is given as [8]:

$$C_{s,e} = \frac{1}{2}\log_2\left(1 + \frac{P * |h_{s,e}|^2}{\sigma_e^2}\right) \quad [32]$$

Secrecy rate of direct transmission is given as [8]:

$$C_s = C_{s,d} - C_{s,e} \quad [33]$$

The final secrecy capacity of direct transmission is given as [8]:

$$C_{final} = \max(C_s, 0)$$

[34]

5.2 Analysis of DF and AF Relaying Schemes with Single Relay

5.2.1 Secrecy Capacity Analysis of DF Relaying Scheme

In decode and forward (DF) relaying, relay decodes the received information signal, re-encode it and transmits to destination. Arrived signals at the destination and eavesdropper are given in equation [6] and [7].

SNR of the signal arrived at the relay is given as [8]:

$$SNR_{s,r} = \frac{P_s * |h_{s,r}|^2}{\sigma_r^2}$$

[35]

where P_s is the power transmitted by the transmitter node, $h_{s,r}$ is the rayleigh channel gain of transmitter to helper and σ_r^2 is AWGN noise variance at the relay.

SNR of the signal arrived at the destination is given as [8]:

$$SNR_{r,d} = \frac{P_r * |h_{r,d}|^2}{\sigma_d^2}$$

[36]

where P_r is the power transmitted by the helper node, $h_{r,d}$ is the rayleigh channel gain of relay to destination and σ_d^2 is AWGN noise variance at the destination.

SNR of the signal arrived at the eavesdropper is given as [8]:

$$SNR_{r,e} = \frac{P_r * |h_{r,e}|^2}{\sigma_e^2}$$

[37]

where P_r is the transmitted power of relay node, $h_{r,e}$ is the rayleigh channel gain of relay to eavesdropper and σ_e^2 is AWGN noise variance at the eavesdropper.

[38]

The instantaneous channel capacity of source to relay according to Shannon's theorem is given as [8]:

$$C_{s,r} = \frac{1}{2}\log_2\left(1 + \frac{P_s * |h_{s,r}|^2}{\sigma_r^2}\right)$$

[39]

The instantaneous channel capacity of relay to destination is given as [8]:

$$C_{r,d} = \frac{1}{2}\log_2\left(1 + \frac{P_r * \left|h_{r,d}\right|^2}{\sigma_d^2}\right)$$

[40]

The instantaneous channel capacity of relay to eavesdropper is given as [8]:

$$C_{r,e} = \frac{1}{2}\log_2\left(1 + \frac{P_r * \left|h_{r,e}\right|^2}{\sigma_e^2}\right)$$

[41]

Secrecy rate of DF relaying scheme is given as [8] :

$$C_s = \min\left(C_{s,r}, C_{r,d}\right) - C_{r,e}$$

[42]

The final secrecy capacity of decode and forward relaying scheme is given as [8]:

$$C_{final} = \max(C_s, 0)$$

[43]

5.2.2 Secrecy Capacity Analysis of AF Relaying Scheme

In amplify and forward (AF) relaying, relay amplifies the received information signal and transmits to legitimate receiver. Arrived signals at the destination and eavesdropper are given in equations [8] and [9].

SNR of the signal arrived at the relay is given as [11]:

$$SNR_{s,r} = \frac{P_s * \left|h_{s,r}\right|^2}{\sigma_r^2}$$

where P_s is the transmitted power of source node, $h_{s,r}$ is the rayleigh channel gain of source to relay and σ_r^2 is AWGN noise variance at the relay.

SNR of the signal arrived at the destination is given as [11]:

$$SNR_{r,d} = \frac{P_r * \left|h_{r,d}\right|^2}{\sigma_d^2}$$

where P_r is the transmitted power of relay node, $h_{r,d}$ is the rayleigh channel gain of relay to destination and σ_d^2 is AWGN noise variance at the destination.

The overall SNR of the signal which is arrived at the destination via relays is given as [11]:

$$SNR_{s,r,d} = \frac{SNR_{s,r} * SNR_{r,d}}{SNR_{s,r} + SNR_{r,d}}$$

[44]

SNR of the signal arrived at the eavesdropper is given as [8]:

$$SNR_{r,e} = \frac{P_r * \left|h_{r,e}\right|^2}{\sigma_e^2}$$

where P_r is the power transmitted by relay node, $h_{r,e}$ is the rayleigh channel gain of relay to eavesdropper and σ_e^2 is AWGN noise variance at the eavesdropper.

According to Shannon's theorem the channel capacity is given as [8]:

$$C = \frac{1}{2}\log_2(1 + SNR)$$

The instantaneous channel capacity of source to destination via relay is given as [8]:

$$C_{s,r,d} = \frac{1}{2}\log_2\left(1 + SNR_{s,r,d}\right)$$

The instantaneous channel capacity of relay to eavesdropper is given as [8]:

$$C_{r,e} = \frac{1}{2}\log_2\left(1 + \frac{P_r * \left|h_{r,e}\right|^2}{\sigma_e^2}\right)$$

The final secrecy capacity of amplify and forward relaying scheme is given as [8]:

$$C_{final} = \max(C_{s,r,d} - C_{r,e}, 0)$$

5.2.3 Simulation Study and Analysis

MATLAB simulation has been performed to investigate the effect cooperative strategies on the relaying schemes for single relayed linear cooperative wireless network. Simulation results obtained using Monto Carlo simulation are shown below, to validate the improvement of secrecy rate.

Here for simplicity, here we have taken equal power for source and helper i.e. total power P=1W is divided equally between source and relay. i.e. P_s=0.5W and P_r=0.5W. The source node is taken as a reference node and it is fixed at origin. Relay, destination and eavesdropper are fixed at the positions 6Km, 20Km and 15Km from the source respectively.

Table 5.1 Simulation parameters for single relay case:

Parameters	Specification
Number of bits	10^3
Path loss index	2
Modulation	QPSK
Number of relays	1
Relays network topology	Linear topology
Channel	Flat Rayleigh fading

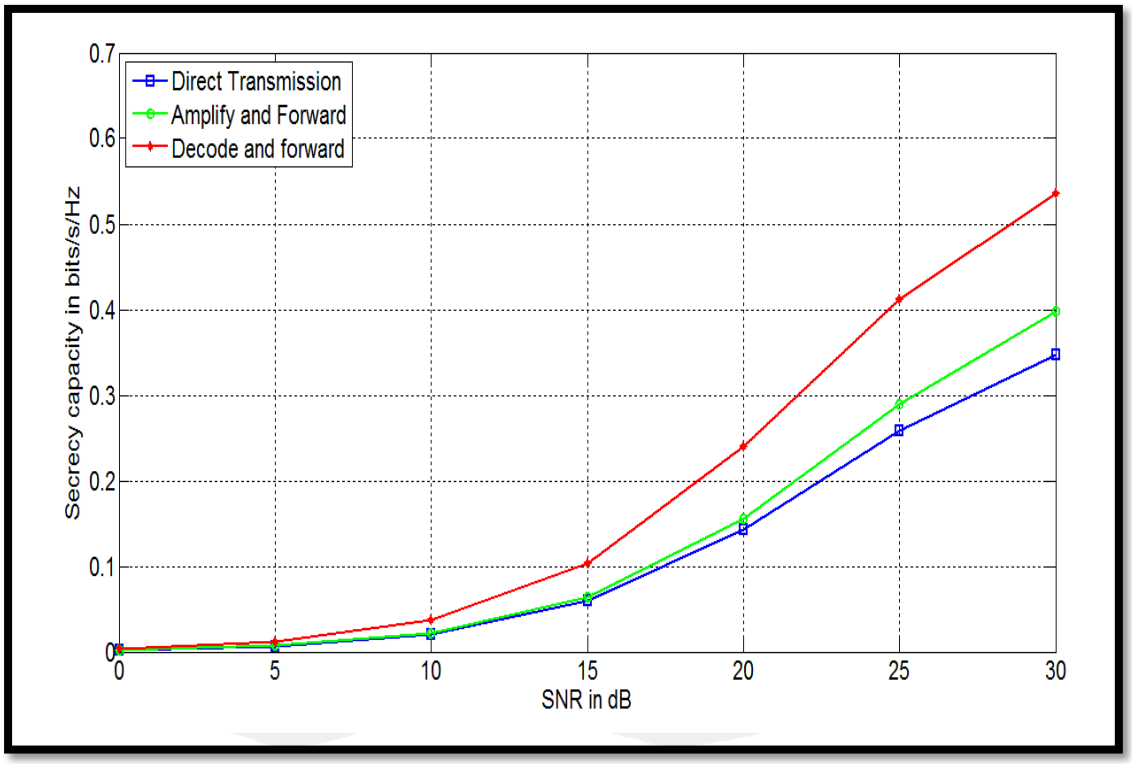

Fig 5.3: Secrecy capacity of basic relaying schemes as a function of signal to noise ratio (dB) for single relay

Table 5.2 Comparison table of basic relaying schemes at SNR=25dB in the case of single relay:

Relaying scheme	Secrecy capacity(bits/s/hz)
Decode and Forward (DF)	~0.41
Amplify and Forward (AF)	~0.29
Direct transmission	~0.26

From Table 5.2, we can observe that cooperative relaying schemes showed improved performance in terms of secrecy capacity. At low SNR values, relaying schemes and direct transmission are showed almost equal

performance. At SNR=25dB, Decode and Forward showed the improvement of 0.15 BPCU (Bits per Channel Unit) and Amplify and Forward showed the performance of 0.03 BPCU than the direct transmission.

5.3 Analysis of DF and AF Relaying Schemes with Multiple Relays

5.3.1 Secrecy Capacity Analysis of DF Relaying Scheme:

In decode and forward (DF) relaying, all the N relays decodes the arrived information signal, re-encode it and transmits to destination. Arrived signals at the destination and eavesdropper are given as [11]:

$$Y_{r_i,d} = \sqrt{P_{r_i}} H^*_{r_i,d} S_{DF} + n_d$$

$$Y_{r_i,e} = \sqrt{P_{r_i}} H^*_{r_i,e} S_{DF} + n_e$$

Where P_{r_i} is the power transmitted by the i^{th} relay node, $H_{r_i,d}$ is the rayleigh channel fading coefficient of i^{th} relay-destination link, $H_{r_i,e}$ is the rayleigh channel fading coefficient of i^{th} relay-eavesdropper link, S_{DF} is the re-encoded signal and n_d, n_e are the AWGN noises with zero mean and variance as 1 at destination and eavesdropper respectively.

SNR of the signal arrivedd at the i^{th} relay is given as [8]:

$$SNR_{s,r_i} = \frac{P_s * \left|h_{s,r_i}\right|^2}{\sigma^2_{r_i}}$$

where P_s is the power transmitted by the source node, h_{s,r_i} is the rayleigh channel gain of source to i^{th} relay and $\sigma^2_{r_i}$ is AWGN noise variance at the i^{th} relay.

SNR of the signal arrived at the destination is given as [8]:

$$SNR_{r_i,d} = \frac{P_{r_i} * \left|h_{r_i,d}\right|^2}{\sigma^2_d}$$

where P_{r_i} is the transmitted power of i^{th} relay node, $h_{r_i,d}$ is the rayleigh channel gain of i^{th} relay-destination link and σ^2_d is AWGN noise variance at the destination.

SNR of the signal arrived at the eavesdropper is given as [8]:

$$SNR_{r_i,e} = \frac{P_{r_i} * \left|h_{r_i,e}\right|^2}{\sigma^2_e}$$

where P_{r_i} is the transmitted power of i^{th} relay node, $h_{r_i,e}$ is the rayleigh channel gain of i^{th} relay-eavesdropper link and σ^2_e is AWGN noise variance at the eavesdropper.

According to Shannon's theorem the channel capacity is given as [8]:

$$C = \frac{1}{2}\log_2(1 + SNR)$$

The instantaneous channel capacity of source to relay is given as [8]:

$$C_{s,r} = \frac{1}{2}\log_2\left(1 + \sum_{i=1}^{N} \frac{P_s * \left|h_{s,r_i}\right|^2}{\sigma_{r_i}^2}\right)$$

[45]

The instantaneous channel capacity of relay to destination is given as [8]:

$$C_{r,d} = \frac{1}{2}\log_2\left(1 + \sum_{i=1}^{N} \frac{P_{r_i} * \left|h_{r_i,d}\right|^2}{\sigma_d^2}\right)$$

[46]

The instantaneous channel capacity of relay to eavesdropper is given as [8]:

$$C_{r,e} = \frac{1}{2}\log_2\left(1 + \sum_{i=1}^{N} \frac{P_{r_i} * \left|h_{r_i,e}\right|^2}{\sigma_e^2}\right)$$

[47]

Secrecy rate of DF relaying scheme for multiple relays is given as [8]:

$$C_s = \min\left(C_{s,r}, C_{r,d}\right) - C_{r,e}$$

The final secrecy capacity of decode and forward relaying scheme for multiple relays is given as [8]:

$$C_{final} = \max(C_s, 0)$$

5.3.2 Secrecy Capacity Analysis of AF Relaying Scheme

In amplify and forward (AF) relaying, all the N relays amplifies the arrived information signal and forwards to destination. Arrived signals at the destination and eavesdropper are given as [11]:

$$Y_{r_i,d} = \sqrt{P_{r_i}} H_{r_i,d}^* S_{AF} + n_d$$

$$Y_{r_i,e} = \sqrt{P_{r_i}} H_{r_i,e}^* S_{AF} + n_e$$

where $S_{AF} = \left(\frac{Y_{s,r_i} H_{s,r_i}^*}{\sqrt{P_{r_i}}\left|H_{s,r_i}\right|^2}\right)$ is the amplified signal by the i^{th} relay , P_{r_i} is the power transmitted by i^{th} relay node, $H_{r_i,d}$ is the rayleigh channel fading coefficient of i^{th} relay-destination link, $H_{r_i,e}$ is the rayleigh channel coefficient of i^{th} relay-eavesdropper link and n_d, n_e are the AWGN noises with zero mean and variance as 1 at destination and eavesdropper respectively

SNR of the signal arrived at the i^{th} relay is given as [11]:

$$SNR_{s,r_i} = \frac{P_s * \left|h_{s,r_i}\right|^2}{\sigma_{r_i}^2}$$

where P_s is the power transmitted by the source node, $h_{s,r}$ is the rayleigh channel gain of transmitter-helper and σ_r^2 is AWGN noise variance at the relay.

SNR of the signal arrived at the destination from i^{th} relay is given as [11]:

$$SNR_{r_i,d} = \frac{P_{r_i} * \left|h_{r_i,d}\right|^2}{\sigma_d^2}$$

where P_{r_i} is the power transmitted by i^{th} relay node, $h_{r_i,d}$ is the rayleigh channel gain of i^{th} relay-destination link and σ_d^2 is AWGN noise variance at the destination.

The overall SNR of the signal which is arrived at the destination via i^{th} relay is given as [11]:

$$SNR_{s,r_i,d} = \frac{SNR_{s,r_i} * SNR_{r_i,d}}{SNR_{s,r_i} + SNR_{r_i,d}}$$

SNR of the signal arrived at the eavesdropper from i^{th} relay is given as [8]:

$$SNR_{r_i,e} = \frac{P_{r_i} * \left|h_{r_i,e}\right|^2}{\sigma_e^2}$$

where P_r is the power transmitted by relay node, $h_{r,e}$ is the rayleigh channel gain of relay-eavesdropper link and σ_e^2 is AWGN noise variance at the eavesdropper.

The instantaneous channel capacity of source to destination via relay according to Shannon's theorem is given as [8]:

$$C_{s,r,d} = \frac{1}{2}\log_2\left(1 + \sum_{i=1}^{N} SNR_{s,r_i,d}\right)$$

The instantaneous channel capacity of relay to eavesdropper according to Shannon's theorem is given as [8]:

$$C_{r,e} = \frac{1}{2}\log_2\left(1 + \sum_{i=1}^{N} \frac{P_{r_i} * \left|h_{r_i,e}\right|^2}{\sigma_e^2}\right)$$

The final secrecy capacity of amplify and forward relaying scheme for multiple relays is given as [8]:

$$C_{final} = \max(C_{s,r,d} - C_{r,e}, 0)$$

5.3.3 Simulation Study and Analysis

MATLAB simulation has been performed to investigate the effect cooperative strategies on the relaying schemes for multiple relayed linear cooperative wireless network. Simulation results obtained using Monto Carlo simulation are shown below, to validate the improvement of secrecy rate.

Here for simplicity, here we have taken equal power for both source and helper, i.e. total power P=1W is divided equally between source and helper. i.e. P_s=0.5W and P_r=0.5W. The source node is taken as a reference node and it is fixed at origin. Relay, destination and eavesdropper are fixed at the positions 6Km, 20Km and 15Km from the source respectively.

Table 5.3 Simulation parameters for multiple relays case:

Parameters	**Specification**
Number of bits	10^3
Path loss index	2
Modulation	QPSK
Number of relays	3
Relays network topology	Linear topology
Channel	Flat Rayleigh fading

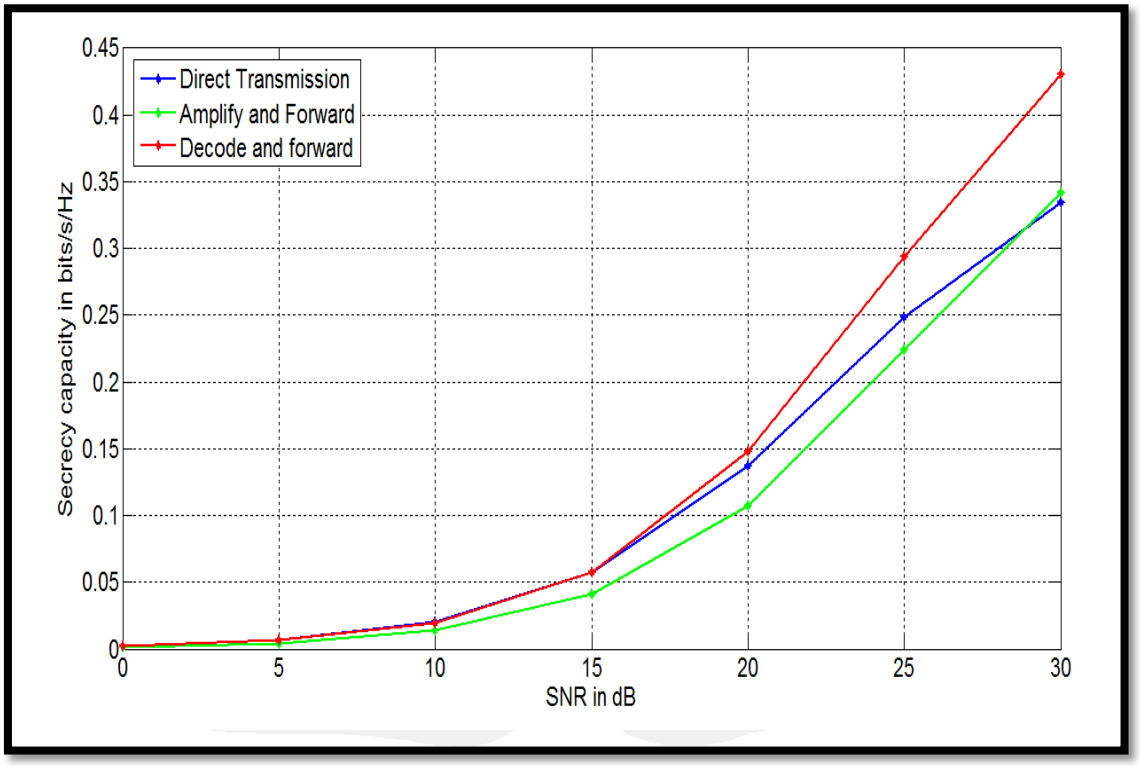

Fig 5.4: Secrecy capacity of basic relaying schemes as a function of signal to noise ratio (dB) for multiple relays

Table 5.4: Comparison table of basic relaying schemes at SNR=25dB in the case of multiple relays:

Relaying scheme	**Secrecy capacity(bits/s/hz)**
Decode and Forward (DF)	~0.29
Amplify and Forward (AF)	~0.225
Direct transmission	~0.26

From Table 5.4, we can observe that, as we increase the number of relays, secrecy capacity of relaying schemes is decreasing because of reduction in channel capacity of source to destination link. At low SNR values, relaying schemes and direct transmission are showed almost equal performance. At SNR=25dB, Decode and Forward showed the improvement of 0.03 BPCU than the direct transmission and Amplify and Forward showed the decrease in secrecy capacity by 0.045 BPCU than direct transmission.

5.4 Analysis of DF and AF Relaying Schemes with Optimal Relay

5.4.1 Secrecy Capacity Analysis of DF Relaying Scheme

To improve the performance of the cooperative wireless network, an optimal relay which is having high SNR at the particular relay needs to be selected. Consider out of N relays i^{th} relay is selected as a best relay. The capacity of source to destination via relays of DF transmission is the minimum of the capacities of source to relay and relay to destination, which is given as [7]:

$$C_{s,r_i,d}^{DF} = \min(C_{s,r_i}, C_{r_i,d}) \quad [48]$$

Where C_{s,r_i} and $C_{r_i,d}$ are the channel capacities of source to i^{th} relay and i^{th} relay to destination which are defined as [7]:

$$C_{s,r_i} = \log_2\left(1 + \frac{P_s * \left|h_{s,r_i}\right|^2}{\sigma_{r_i}^2}\right) \quad [49]$$

and

$$C_{r_i,d} = \log_2\left(1 + \frac{P_{r_i} * \left|h_{r_i,d}\right|^2}{\sigma_d^2}\right) \quad [50]$$

When relay is transmitting the signal, eavesdropper overhears the transmitted information due to openness of wireless medium. The channel capacity of i^{th} relay to eavesdropper is given as [7]:

$$C_{r_{i,e}}^{DF} = \log_2\left(1 + \frac{P_{r_i} * \left|h_{r_i,e}\right|^2}{\sigma_e^2}\right)$$

The secrecy capacity of DF relaying scheme is given as [7]:

$$C_s^{DF} = C_{s,r_i,d}^{DF} - C_{r_{i,e}}^{DF}$$

The relay which gives maximum secrecy capacity can be selected as an optimal relay and it is selected based on the following equation [7]:

$$R_{opt} = \max(C_i^{DF})$$

5.4.2 Secrecy Capacity Analysis of AF Relaying Scheme

To improve the performance of the cooperative wireless network, an optimal relay which is having high SNR at the particular relay needs to be selected. Consider out of N relays i^{th} relay is selected as a best relay. The channel gain of source to destination via relays of AF transmission is the harmonic mean of the channel gain of source to relay and relay to destination, which is given as [6]:

$$\left|h_{s,r_i,d}\right|^2 = \frac{\left|h_{s,r_i}\right|^2 * \left|h_{r_i,d}\right|^2}{\left|h_{s,r_i}\right|^2 + \left|h_{r_i,d}\right|^2} \quad [51]$$

Hence the channel capacity of source to destination via optimal relay for AF transmission in the case of optimal relay is given as [6]:

$$C_{s,r_i,d}^{AF} = \log_2\left(1 + \frac{P_{r_i} * \left|h_{s,r_i,d}\right|^2}{\sigma_d^2}\right)$$

When relay is transmitting the signal, eavesdropper overhears the transmitted information due to openness of wireless medium. The channel capacity of optimal relay to eavesdropper is given as [6]:

$$C_{r_{i,e}}^{AF} = \log_2\left(1 + \frac{P_{r_i} * \left|h_{r_i,e}\right|^2}{\sigma_e^2}\right)$$

The secrecy capacity of AF relaying scheme is given as [6]:

$$C_s^{AF} = C_{s,r_i,d}^{AF} - C_{r_{i,e}}^{AF}$$

The relay which gives maximum secrecy capacity can be selected as an optimal relay and it is selected based on the following equation [6]:

$$R_{opt} = \max(C_i^{AF})$$

5.4.3 Simulation Study and Analysis

MATLAB simulation has been performed to investigate the effect cooperative strategies on the relaying schemes in the case of an optimal relay for linear cooperative wireless network. Simulation results obtained using Monto Carlo simulation are shown below, to validate the improvement of secrecy rate.

Here for simplicity, here we have taken equal power for both source and relay, i.e. total power P=1W is divided equally between source and relay. i.e. P_s=0.5W and P_r=0.5W. The source node is taken as a reference node and it is fixed at origin. Relay, destination and eavesdropper are fixed at the positions 6Km, 20Km and 15Km from the source respectively.

Table 5.5 Simulation parameters for optimal relay case:

Parameters	**Specification**
Number of bits	10^3
Path loss index	2
Modulation	QPSK
Number of relays	3
Relays network topology	Linear topology
Channel	Flat Rayleigh fading

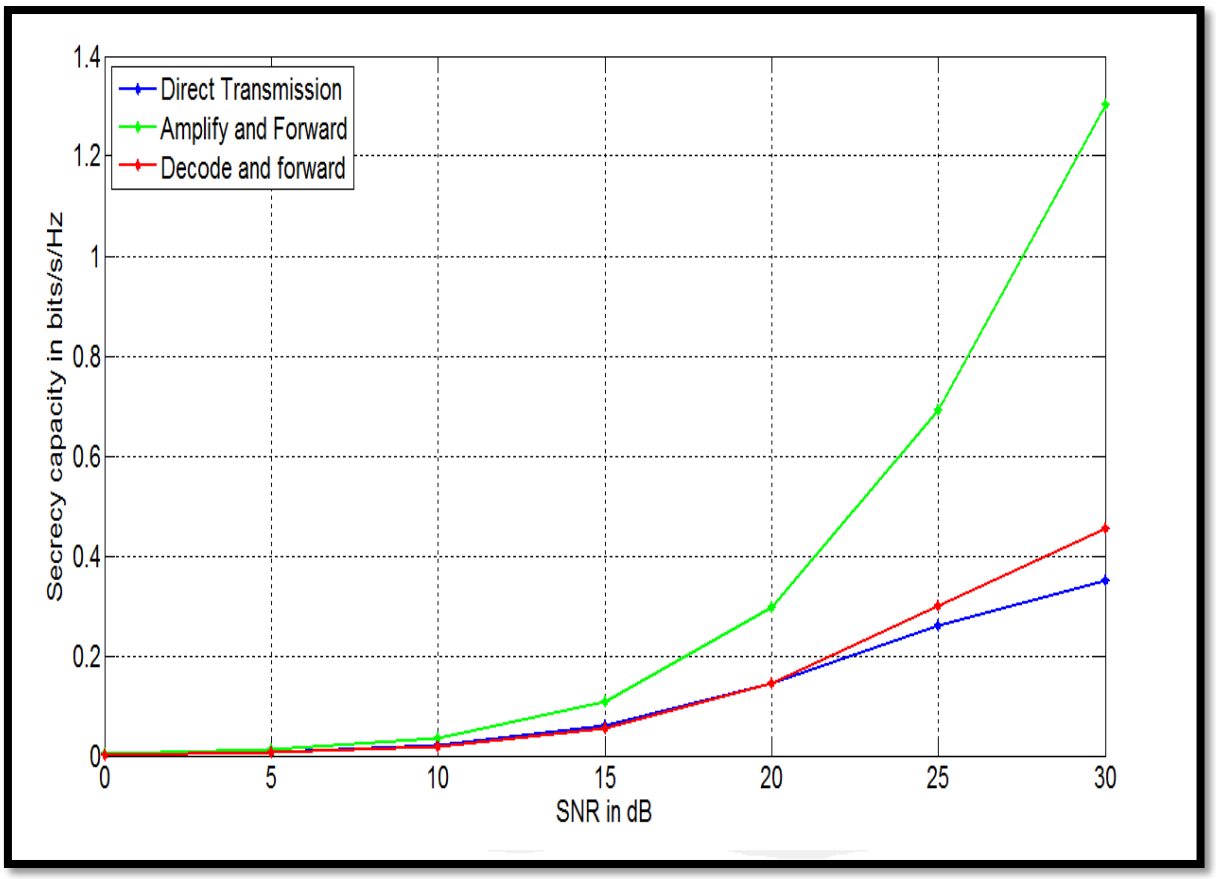

Fig 5.5: Secrecy capacity of basic relaying schemes as a function of signal to noise ratio (dB) for optimal relay

Table 5.6 Comparison table of basic relaying schemes at SNR=25dB in the case of optimal relay:

Relaying scheme	**Secrecy capacity(bits/s/hz)**
Decode and Forward (DF)	~0.31
Amplify and Forward (AF)	~0.7
Direct transmission	~0.26

From Table 4, we can observe that in the case of optimal relay amplify and forward showed the better performance compared to decode and forward and direct transmission. For Amplify and forward relaying, we can also observe the improvement in secrecy capacity by 0.41 BPCU than the single relay case. At low SNR values, relaying schemes and direct transmission are showed almost equal performance. At SNR=25dB, Decode and Forward showed the improvement of 0.05 BPCU than the direct transmission and Amplify and Forward showed the decrease in secrecy capacity by 0.44 BPCU than direct transmission.

5.5 Analysis of AF Relaying Scheme with Increase in Number of relays

5.5.1 Secrecy Capacity Analysis of AF Relaying Scheme

In this subsection we are going to show the improvement in physical layer security by selecting the single best relay to transmit the source information using AF relaying scheme. For comparative analysis, we consider the direct transmission where the transmitter transmits its information to the legitimate receiver without the help of relays and at the same time eavesdropper overhears the source information due to broadcast nature. As explained in system model, secrecy rate is given as [25]:

$$C_s = \log_2\left(1 + \frac{P\left|h_{s,d}\right|^2}{\sigma_d^2}\right) - \log_2\left(1 + \frac{P\left|h_{s,e}\right|^2}{\sigma_e^2}\right) \quad [51]$$

Secrecy capacity is given as [25]:

$$C_s^{capacity} = \max(C_s, 0)$$

Secrecy capacity is analysed for different main to eavesdropper ratio which is given as [25]:

$$MER = \frac{\sigma_{s,d}^2}{\sigma_{s,e}^2} \quad [52]$$

where $\sigma_{s,d}^2$ is average main channel gain and $\sigma_{s,e}^2$ is the average eavesdropper channel gain.

In AF relaying scheme, an optimal relay will be selected to amplify and forward the source information and it is selected based on the given expression shown below [25]:

$$R_{opt} = \max\left(\frac{\left|h_{s,r_i}\right| * \left|h_{r_i,d}\right|}{\left|h_{s,r_i}\right| + \left|h_{r_i,d}\right|}\right) \quad [53]$$

where i belongs to the relays set.

5.5.1.1 Simulation Study and Analysis

MATLAB simulation has been performed to investigate the effect of cooperative strategies on the proposed relaying schemes for linear cooperative wireless network. Simulation results obtained using Monto Carlo simulation are shown below, to validate the improvement of secrecy rate for different number of relays

Here we have taken equal power for both source and helper, i.e. total power P=1W is divided equally between source and relay. i.e. P_s=0.5W and P_r=0.5W.

Table 5.7: Simulation parameters of AF relaying secrecy capacity with increase in number of relays

Parameters	**Specification**
Number of bits	10^3
Path loss index	2
Modulation	QPSK
Number of relays	2,4,8
Relays network topology	Linear topology
Channel	Flat Rayleigh fading

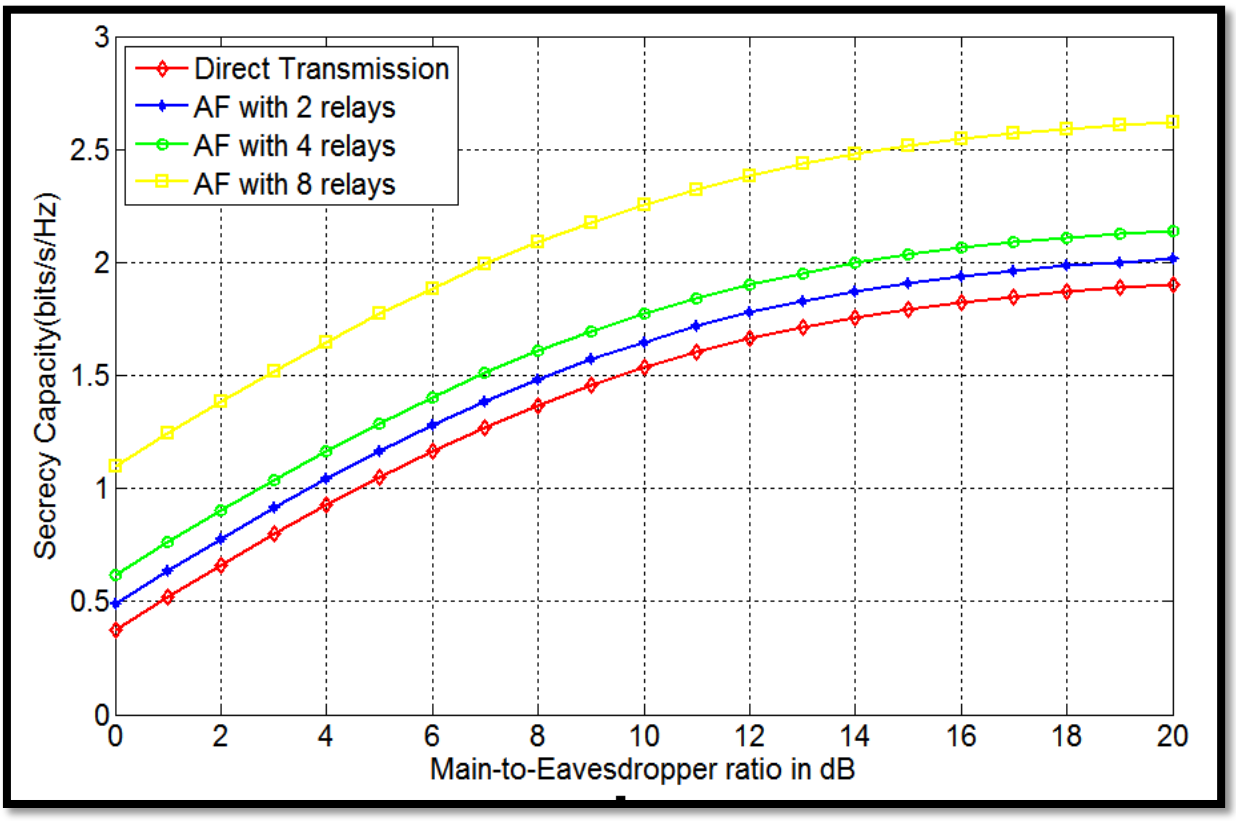

Fig 5.6: Secrecy capacity of Amplify and forward relaying scheme as a function of Main to Eavesdropper ratio (dB)

Table 5.8: Comparison table of AF relaying secrecy capacity with increase in number of relays at MER=20dB

Relaying scheme	**No of relays**	**Secrecy Capacity (Bits/s/Hz)**
Amplify and Forward	2	~2.0
	4	~2.15
	8	~2.65
Direct Transmission		~1.8

From Table 5, we can observe that, as we increase the number of relays, secrecy capacity of amplify and forward relaying scheme showed improved performance. At MER=20dB, in the entire cases cooperative relaying scheme outperforms direct transmission. We can also observe that in the case of 8 relays there is a gain of 0.5 BPCU than 4 relays and gain of 0.65 BPCU than 2 relays.

5.5.2 Intercept Probability Analysis of AF Relaying Scheme

In this subsection we are introducing another performance parameter of cooperative communication i.e. intercept probability which is defined as the probability of occurrence of an intercept event. As we already know intercept event occurs when secrecy capacity falls below zero.

For comparative analysis, we considered direct transmission. Intercept probability of direct transmission is given as [25]:

$$P_{intercept}^{direct} = Pr\left(C_{s,d}^{direct} < C_{s,e}^{direct}\right)$$

$$= Pr\left(\left|h_{s,d}\right|^2 < \left|h_{s,e}\right|^2\right) \qquad [54]$$

$$= \frac{\sigma_{s,e}^2}{\sigma_{s,e}^2+\sigma_{s,d}^2}$$

In the case of Amplify and Forward (AF) relaying, intercept probability is defined as [25]:

$$P_{intercept}^{AF} = Pr\left(maxC_i^{AF} < 0\right)$$

$$= \prod_{i=1}^{N} Pr\left(\left|h_{r_i,d}\right|^2 < \left|h_{r_i,e}\right|^2\right)$$

$$= \prod_{i=1}^{N} \frac{\sigma_{r,e}^2}{\sigma_{r,e}^2+\sigma_{r,d}^2} \qquad [55]$$

Where N represents the number of relays, $\sigma_{s,d}^2$ is average main channel gain, $\sigma_{s,e}^2$ is the average eavesdropper

channel gain, $\sigma_{r,d}^2$ is average channel gain of relay to destination and $\sigma_{r,e}^2$ is the average channel gain of relay to eavesdropper.

5.5.2.1 Simulation Study and Analysis

MATLAB simulation has been performed to investigate the effect of cooperative strategies on the proposed relaying schemes for linear cooperative wireless network. Simulation results obtained using Monto Carlo simulation are shown below, to validate the improvement of secrecy rate for different number of relays

Here we have taken equal power for both relay and source, i.e. total power P=1W is divided equally between source and relay. i.e. P_s=0.5W and P_r=0.5W.

Table 5.9: Simulation parameters of AF relaying intercept probability with increase number of relays

Parameters	**Specification**
Number of bits	10^3
Path loss index	2
Modulation	QPSK
Number of relays	2,4,8
Relays network topology	Linear topology
Channel	Flat Rayleigh fading

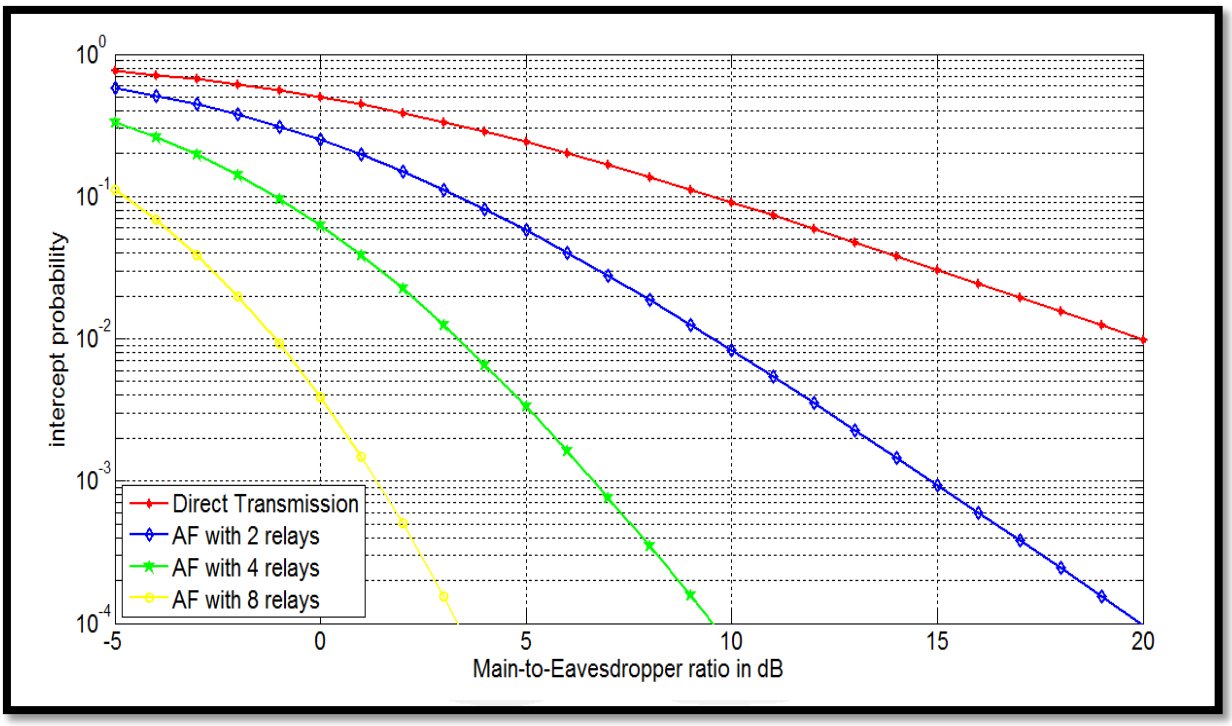

Fig 5.7: Intercept Probability of Amplify and forward relaying schemes as a function of Main to Eavesdropper ratio (dB)

Table 5.10: Comparison Table Of Amplify and Forward Relaying Intercept Probability at MER=5dB with the Increase in Number of Relay

Relaying scheme	No of relays	Intercept Probability
Amplify and Forward	2	<< 0.0001
	6	~0.0035
	8	~0.06
Direct Transmission		~0.25

From Table 6, we can observe that as we increase the number of relays there is a reduction in intercept probability of amplify and forward relaying. At MER=5dB in the entire cases cooperative relaying scheme outperforms direct transmission. In AF relaying, for eight relays there is percentage gain of 94% compared to four relays case and percentage gain of 99.8% compared to two relays case.

5.6 Proposed Work for the Performance Analysis of HDAF Relaying Scheme

5.6.1 Introduction

In this section performance analysis of Hybrid decode-Amplify-Forward (HDAF) is analysed in the presence of single eavesdropper. HDAF is a new adaptive relaying scheme which switches between DF and AF relaying scheme based on the decoding capability of the relay.

HDAF	=	DF	If relay can decode the signal impeccably
	=	AF	else

During cooperative phase, one out of N relays is selected on the basis of three proposed selection schemes, to improve the achievable secrecy rate through cooperation and one more relay is selected from the remaining N-1 relays to operate as a jammer. The cooperative relay operates in either DF or AF mode based on its decoding capability. If the cooperative relay impeccably decodes the received information signal, then it operates in DF mode or else it operates in AF mode.

5.6.2 Secrecy Capacity Analysis of HDAF Relaying Scheme

In hybrid relaying, if relay decodes the signal perfectly ($SNR_{s,r} > threshold$), it operates in DF mode, otherwise i.e. if relay can not able to decode the signal perfectly ($SNR_{s,r} < threshold$), it operates in AF mode. Here threshold is target transmission rate.

The channel capacity of hybrid relaying is defined as [28]:

$$C_{HDAF} = \Pr\left(SNR_{s,r_i} > threshold\right) C_{DF} + \Pr\left(SNR_{s,r_i} < threshold\right) C_{AF} \quad [56]$$

Where C_{DF} is the secrecy capacity of DF relaying scheme and C_{AF} is the secrecy capacity of AF relaying scheme.

$$\Pr\left(SNR_{s,r_i} > threshold\right) \approx 1 - \prod_{i=1}^{N} \exp\left(\frac{-threshold}{SNR_{s,r_i}}\right) \quad [57]$$

$$\Pr\left(SNR_{s,r_i} < threshold\right) \approx \prod_{i=1}^{N} \exp\left(\frac{-threshold}{SNR_{s,r_i}}\right) \quad [58]$$

5.6.3 Simulation Study and Analysis:

MATLAB simulation has been performed to investigate the effect of jamming performance and cooperative strategies on the proposed relaying schemes for linear cooperative wireless network. Simulation results obtained using Monto Carlo simulation are shown below, to validate the improvement of secrecy rate for different relay and jamming selection schemes.

To illustrate the effect of jamming and advantage of using HDAF relaying scheme, a linear cooperative network was considered in which source, destination, relays and eavesdropper are placed linearly. The source node is taken as a reference node and it is fixed at origin. The direct paths, source to legitimate receiver(S→D) and source to illegitimate receiver (S→E) links are known. For simplicity, we have allocated equal power to source and relays ($P_s = P_r$) and in order to mitigate the effect of jamming signal at the destination, jamming power is taken as$P_j = P_r/L$. Here we considered L as 100. The parameters chosen for the simulation are given in Table 5.11.

Table 5.11: Simulation parameters for HDAF relaying for different relay and jammer selection schemes

Parameters	**Specification**
Number of bits	10^4
Path loss index	3
Modulation	QPSK
Number of relays	2
Target transmission rate	0.5
Relays network topology	Linear topology
Channel	Flat Rayleigh fading

As the location of relay plays an important role here, we considered two cases, first one is relays placed close to eavesdropper and second one is relays placed close to destination for the 3 proposed relay and jamming selection schemes.

Case (i) Relay close to eavesdropper:

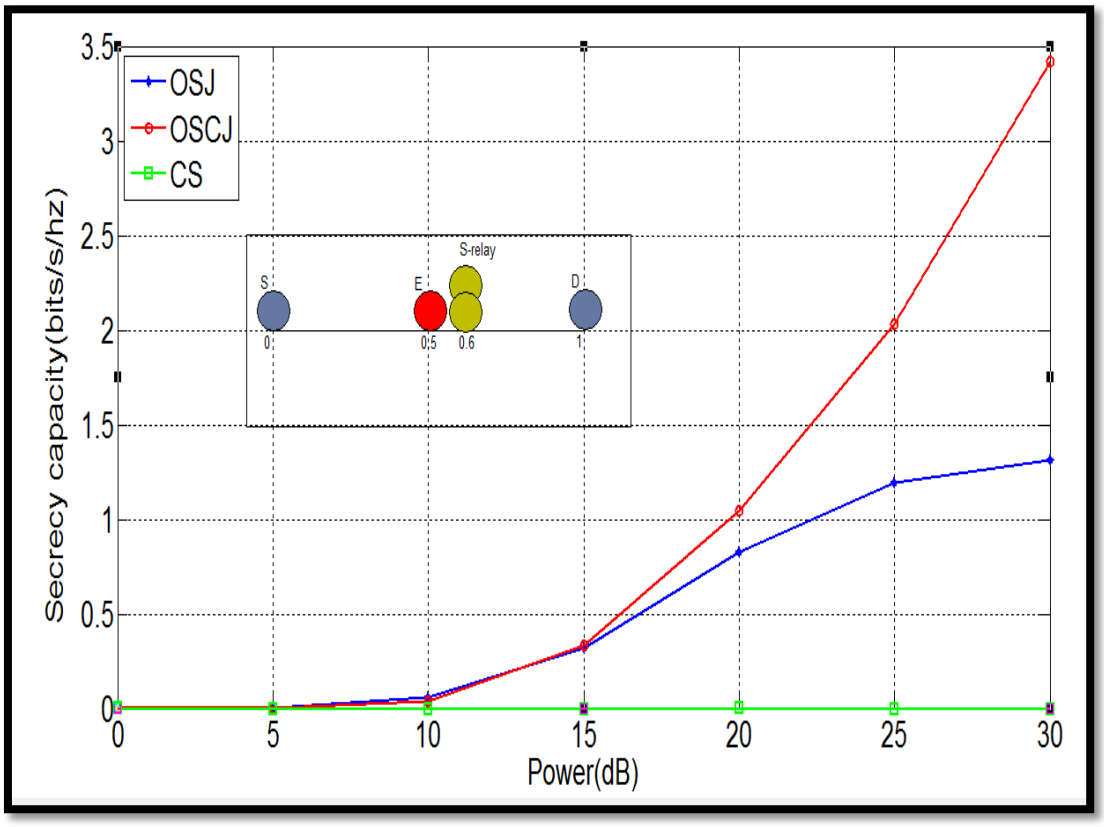

Fig 5.8: Secrecy capacity as a function of total transmit power when relays are located near to eavesdropper

Table 5.12 Comparison table of relay and jammer selection schemes at P=25dB for HDAF relaying when relay located near to eavesdropper:

Relay and jamming selection scheme	Secrecy capacity in bits/s/hz
Conventional selection	0
Optimal selection with jamming	1.22
Optimal selection with control jamming	2

Fig 6 shows the secrecy capacity of the proposed relay and jamming selection schemes with respect to the total transmit power P when relay is located near to eavesdropper. It has been observed that optimal selection with control jamming (OSCJ) outperforms OSJ and CS selection schemes. Optimal selection with jamming showed 1.38BPCU (Bits Per channel Use) gain (at 25 dB) compared to non-jamming selection scheme. For the secrecy capacity of 1 BPCU, control jamming has taken 2.5 dB less power compared to

optimal selection with jamming. Non availability of the jammer in conventional selection leads to zero secrecy rate.

Case (ii) Relay close to destination:

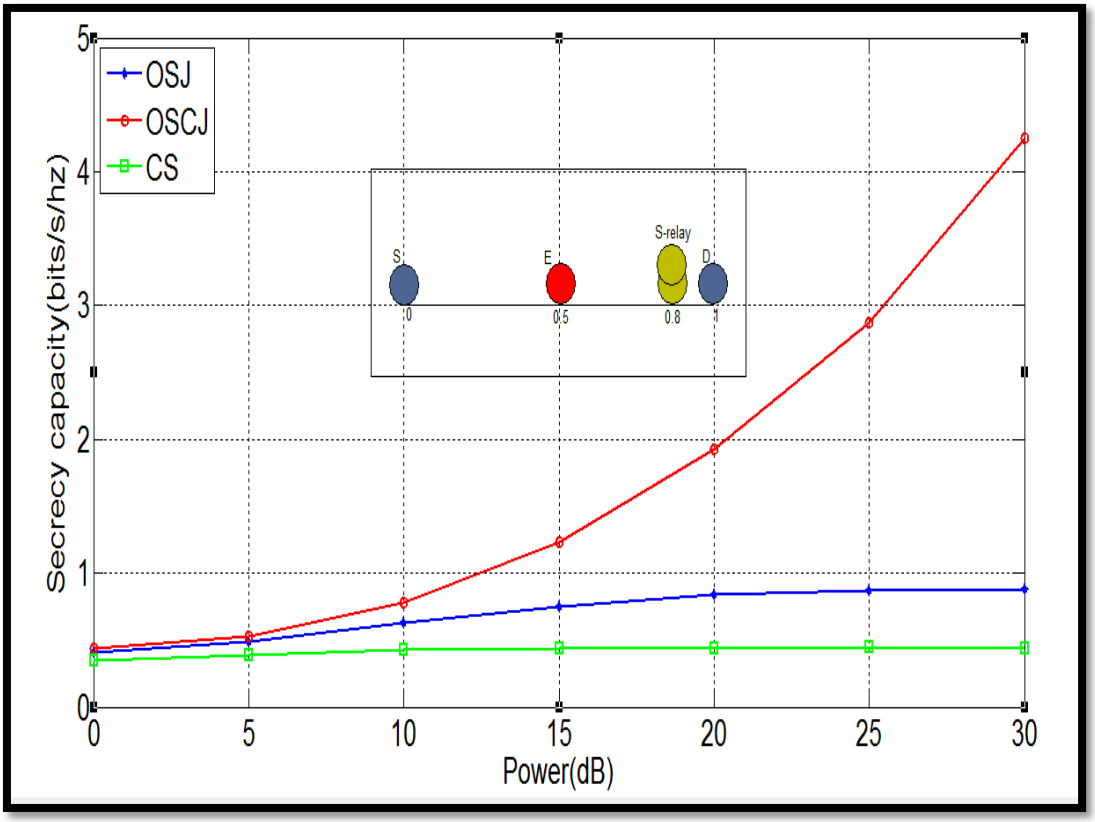

Fig 5.9: Secrecy capacity as a function of total transmit power when relays are located near to the destination

Table 5.13 Comparison table of relay and jammer selection schemes at P=25dB for HDAF relaying when relay located near to destination:

Relay and jamming selection scheme	**Secrecy capacity in bits/s/hz**
Conventional selection	0.4
Optimal selection with jamming	0.9
Optimal selection with control jamming	2.9

Fig 7 shows the secrecy capacity of the proposed relay and jamming selection schemes with respect to the total transmit power P when relay is located near to destination. It has been observed that, for control jamming when the relay is moving towards the destination there has been an improvement in secrecy capacity by 0.9 BPCU (at 25 dB). Since the destination is unaware of the jamming signal, secrecy capacity of optimal selection with jamming decreases by 0.48BPCU. In this case all the selection schemes showed non zero secrecy rate.

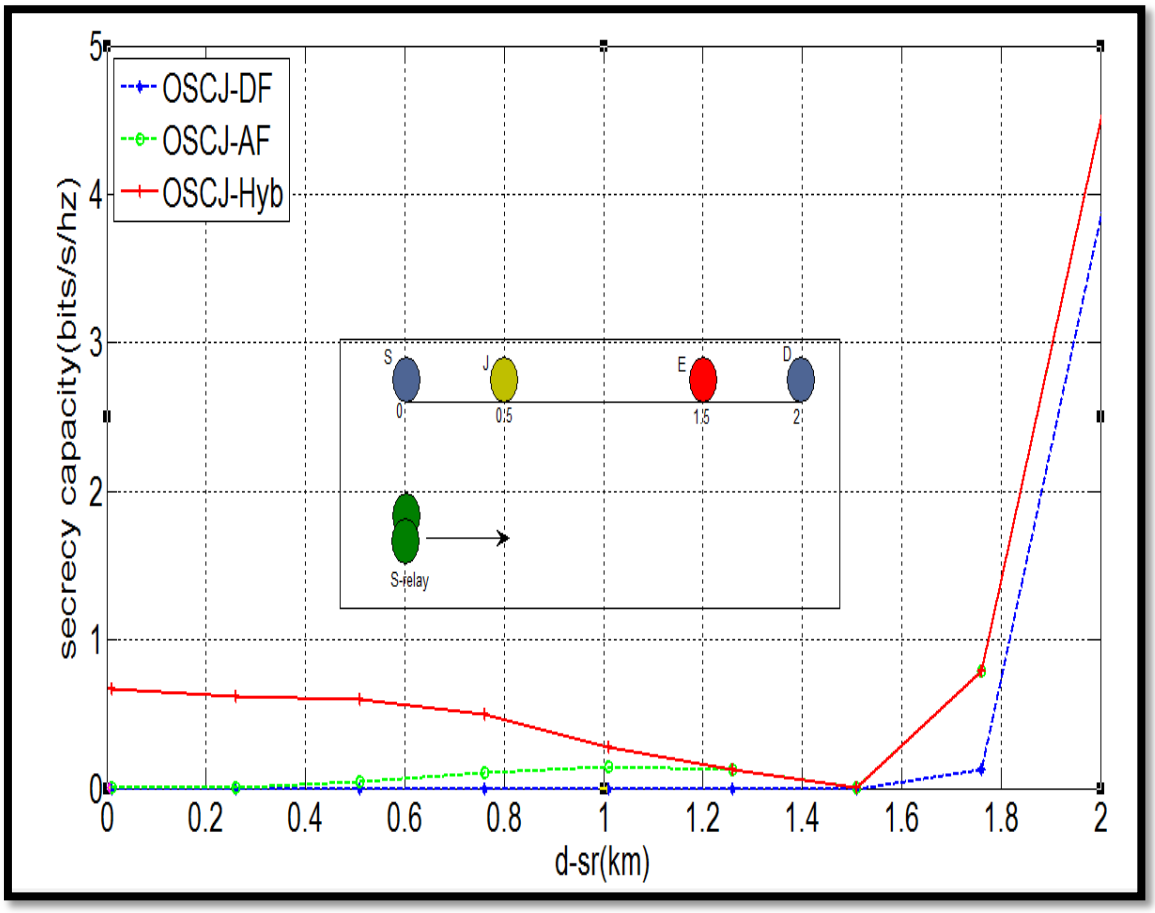

Fig 5.10: Secrecy capacity as a function of source to relay distance

Fig 8 shows the secrecy capacity of control jamming scheme with respect to the source to relay distance (d_sr). In this the position of jammer, eavesdropper and destination are fixed at 0.5km, 1.5km and 2km respectively. It has been observed that HDAF relaying outperforms AF and DF relaying schemes and we can also observe that till the position of the eavesdropper, there has been a decrease in secrecy capacity for HDAF relaying scheme. When relay is located at eavesdropper's position, all the relaying schemes resulted zero secrecy capacity.

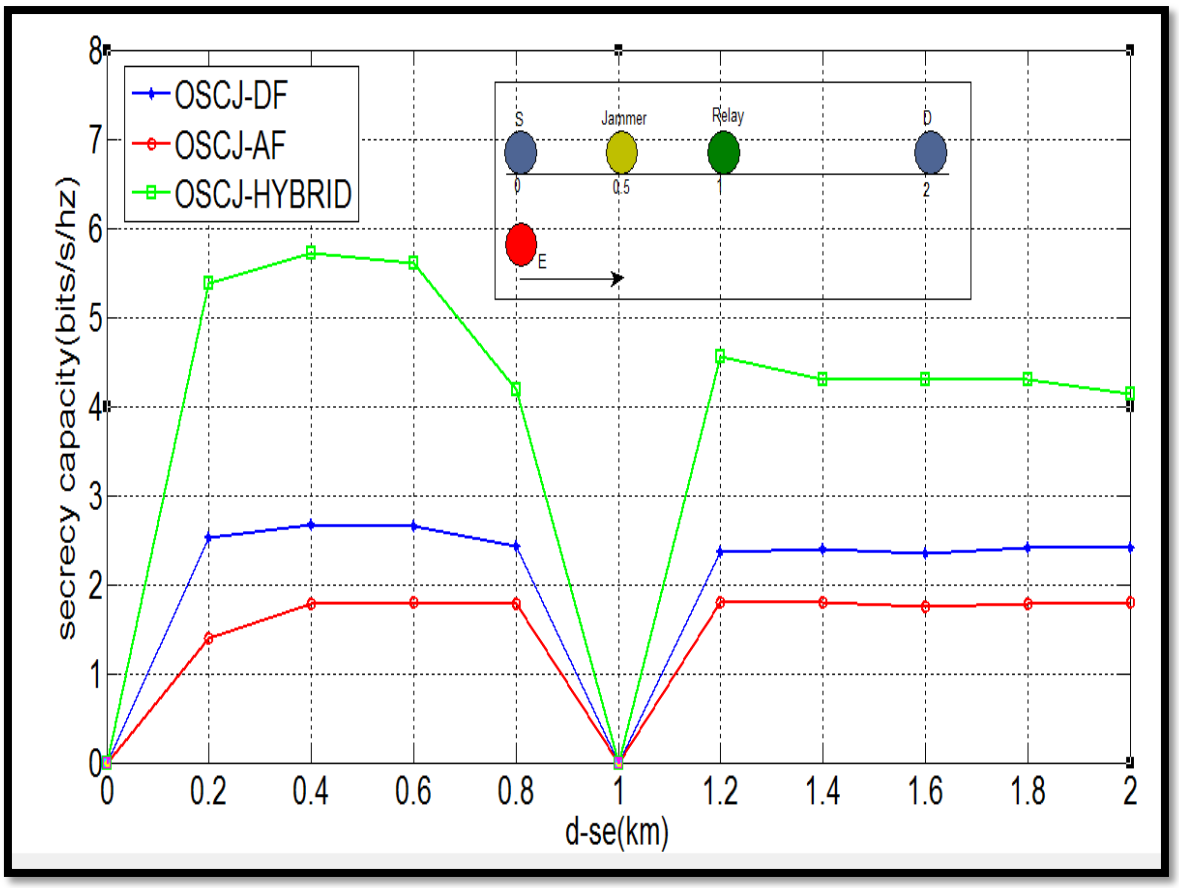

Fig 5.11: Secrecy capacity as a function of source to eavesdropper distance

Fig 9 shows the secrecy capacity of control jamming scheme with respect to the source to eavesdropper distance (d_sr). In this the position of jammer, relay and destination are fixed at 0.5km, 1km and 2km respectively. It has been observed that HDAF relaying outperforms AF and DF relaying schemes. When eavesdropper is moving towards the jammer (i.e. till position 0.5), secrecy capacity of relaying schemes improves due to the interference caused by the jammer to the eavesdropper. When eavesdropper is at the position of the relay, all the relaying schemes showed zero secrecy capacity.

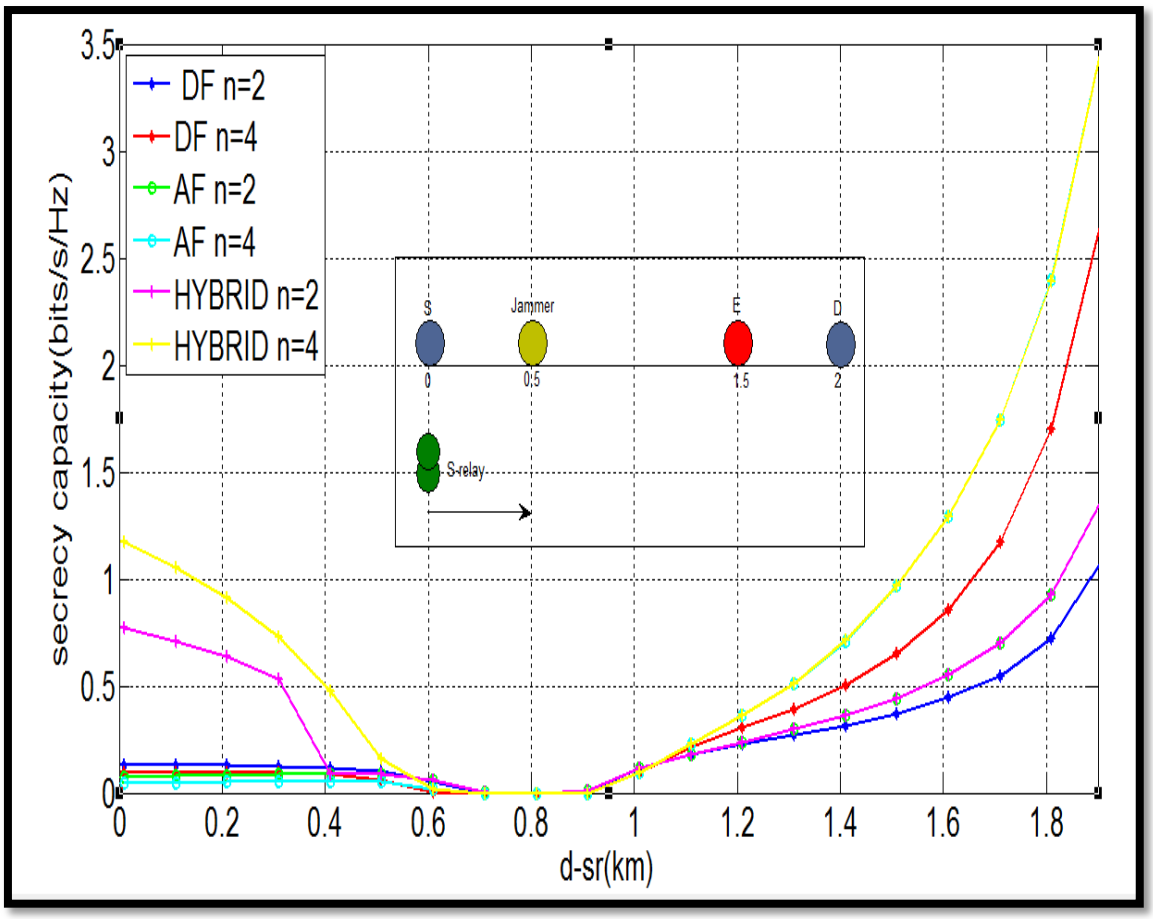

Fig5.12: Secrecy capacity for different path loss indices

Fig 10 shows the secrecy capacity of control jamming scheme for two different path loss indices (n=2 and n=4) with respect to the source to relay distance. In this the position of jammer, eavesdropper and destination are fixed at 0.5km, 1.5km and 2km respectively. It has been observed that HDAF relaying outperforms AF and DF relaying schemes and also the secrecy capacity of each relaying scheme increases, as we increase the path loss index from n=2 to n=4. This analysis has been performed to study the effect of various types of propagation environment on the secrecy capacity.

6

CONCLUSION AND FUTURE SCOPE OF RESEARCH

6.1 Conclusion

Cooperative relaying schemes has many advantages in terms of secrecy capacity and intercept probability when compared to straight transmission. In this work, cooperative communication is simulated for Amplify and Forward, Decode and Forward, Hybrid Decode Amplify Forward relaying schemes for single and multiple helpers. All the simulated results prove that the relaying schemes are better in performance when compared to direct transmission.

In order to get the benefits of both DF and AF relaying schemes, an SNR based hybrid decode-amplify-forward (HDAF) for physical layer security of wireless cooperative network is introduced. Its performance is analyzed in flat Rayleigh fading channel environment with three relay and jammer selection schemes namely conventional selection (without jammer), optimal selection (with jammer) and control jamming. Monte Carlo simulations are carried out and the obtained results are compared for different relay and jammer locations. A study of comparison is made in terms of secrecy rate for the proposed hybrid decode-amplify-forward (HDAF) relaying with the AF and DF relaying schemes. Finally from the simulated comparison study, it has been observed that HDAF scheme outperforms AF and DF schemes and it showed improved performance when the helper is near to the destination. Performance of optimal selection with jamming (OSJ) selection scheme decreases as relay moves towards the destination. We can also observe that control jamming selection achieves more secrecy rate compared to without jamming and with optimal jamming.

6.2 Future Scope

All the relaying schemes are analysed only for single eavesdropper case. Hence further work can be extended to multiple eavesdropper environments.

Since relay is using some of its power for jamming purpose, power required to transmit information signal is reduces. Hence further will be extended to, optimal power allocation subjected to a secrecy rate constraint.

References

[1] A.Nosratinia, T.E.Hunter, and A.Hedayat, “Cooperative communication in wireless networks,” *IEEE Commun. Mag., vol. 42, no. 10, pp. 74–80,Oct. 2004.*

[2] Meier, Andreas, and John S. Thompson. "Cooperative diversity in wireless networks." *3G and Beyond, 2005 6th IEE International Conference on*. IET, 2005.

[3] Nicolas Sklavos, Xinmiao Zhang, “ Wireless security and cryptography” : *Specifications and implementations, CRC press, Inc., Boca Raton, FL, 2007*

[4] Stojanovski, Toni Draganov, and Ninoslav Marina. "Secure Wireless Communications via Cooperative Transmitting." *The Scientific World Journal*2014 (2014).

[5] Dong, Lun, et al. "Amplify-and-forward based cooperation for secure wireless communications." *Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on*. IEEE, 2009.

[6] Torabi, Mohammad, Wessam Ajib, and David Haccoun. "Performance analysis of amplify-and-forward cooperative networks with relay selection over Rayleigh fading channels." *Vehicular Technology Conference, 2009. VTC Spring 2009. IEEE 69th*. IEEE, 2009.

[7] Zhao, Jian, et al. "Cooperative transmission schemes for decode-and-forward relaying." *Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium on*. IEEE, 2007.

[8] Li, Jiangyuan, Athina P. Petropulu, and Steven Weber. "On cooperative relaying schemes for wireless physical layer security." *Signal Processing, IEEE Transactions on* 59.10 (2011): 4985-4997.

[9] Yu, Meng, and Jing Li. "Is amplify-and-forward practically better than decode-and-forward or vice versa?." *Acoustics, Speech, and Signal Processing, 2005. Proceedings. (ICASSP'05). IEEE International Conference on*. Vol. 3. IEEE, 2005.

[10] Debbabi, Naoufel, et al. "Comparison of AF and DF relaying for uplink CDMA communications subject to constant multiple access interference cost. "*Communications and Networking, 2009. ComNet 2009. First International Conference on*. IEEE, 2009.

[11] Yulong Zou, Xianbin Wang, Weiming Shen “Optimal relay selection for physical layer security in cooperative wireless networks” *in IEEE Journal on selecte area of communication, Vol. 31, No. 10,October 2013*

[12] Krikidis, Ioannis, John S. Thompson, and Steve McLaughlin. "Relay selection for secure cooperative networks with jamming." *Wireless Communications, IEEE Transactions on* 8.10 (2009): 5003-5011.

[13] Gurrala, Kiran Kumar, and Susmita Das. "Impact of relay location on the performance of multi-relay cooperative communication." *International Journal of Computer Networks and Wireless Communications* 2.2 (2012): 226-231.

[14] Lun Dong, Zhu Han, Athina P. Petropulu, H. Vincent Poor "Improving physical layer security via cooperative relays" *in IEEE Transaction on signal processing, Vol. 58, No. 3, March 2010.*

[15] Li, Jiangyuan, Athina P. Petropulu, and Steven Weber. "On cooperative relaying schemes for wireless physical layer security." *Signal Processing, IEEE Transactions on* 59.10 (2011): 4985-4997.

[16] Liu, Yupeng, Jiangyuan Li, and Athina P. Petropulu. "Destination assisted cooperative jamming for wireless physical-layer security." *Information Forensics and Security, IEEE Transactions on* 8.4 (2013): 682-694.

[17] Wang, Hui-Ming, et al. "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks." *Information Forensics and Security, IEEE Transactions on* 8.12 (2013): 2007-2020.

[18] Ding, Zhiguo, et al. "Opportunistic relaying for secrecy communications: Cooperative jamming vs. relay chatting." *IEEE Transactions on Wireless Communications* 10.6 (2011): 1725-1729.

[19] An Li, Yizhu Xu, Yuhao Wang and Lihua Sun "Amplify-and-forward-based cooperative jamming strategy, with power allocation for secure communication" *in International journal of communication system (2014).*

[20] Vaibhav Kumar Gupta, Poonam Jindal "Performance analysis of cooperative schemes in eavesdropper assisted relay channel" in *ICTACT Journal of Communication Technology, Vol. 05, No. 02, June 2014.*

[21] Doaa H. Ibrahim, Emad S. Hasaan, Sami A. El-Dolil "A new relay and jammer selection schemes for secure one way cooperative networks" in *Wireless Personal Communication, pp. 1-21,Online First, August 2013*

[22] Hazem Mohammed and Taha A. Khalaf, "Optimal positioning of relay node in wireless cooperative communication networks" in *Computer Engineering Conference, 2013, 9th International, IEEE, 2013.*

[23] Adebo Philip, Eyidayo Adebola and Annamali Annamalai, "On the ergodic secrecy rate of cooperative decode and forward relay networks" in *Millitary Communication Conference, IEEE, 5 pages, Oct 2014,*

[24] Hourani, Hafeth. "An overview of diversity techniques in wireless communication systems." *IEEE ISAC, pp-1200-5* (2004).

[25] Y. Zou, J. Zhu, X. Wang, and V. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Network, vol. 29, no. 1, pp. 42-48, Jan. 2015*.

[26] T. Q. Duong and H.-J. Zepernick, "On the, Performance Gain of Hybrid Decode-Amplify-Forward Cooperative Communications," in *EURASIP Journal on Wireless Communications and Networks, Vol. 2009, 10 pages, 2009.*

[27] T. Duong and H.-J. Zepernick, "Hybrid decode-amplify-forward cooperative communications with multiple relays," in *Proc. IEEE Wireless Communications and Networking Conference (WCNC '09), pp. 1 -6, April 2009.*

[28] Gurrala, Kiran Kumar, and Susmita Das. "Maximized Channel Capacity Based Power Allocation Technique for Multi Relay Hybrid Decode-Amplify-Forward Cooperative Network." *Wireless Personal Communications*: 1-16.

[29] Chen, H., & Liu, J., "Performance analysis of SNR-based hybrid decode-amplify-forward cooperative diversity networks over Rayleigh fading channels" in *IEEE wireless communications and networking conference, Sydney, pp. 1–6, 2010.*

[30] Gurrala, Kiran Kumar, and Susmita Das. "Hybrid decode-amplify-forward (HDAF) scheme in distributed Alamouti-coded cooperative network. "*International Journal of Electronics* ahead-of-print (2014): 1-17.

DISSEMINATION OF WORK:

- Thatha Divya, Kiran Kumar Gurala, Susmita Das.” **Performance Analysis of Hybrid Decode-Amplify-Forward (HDAF) relaying for improving security in cooperative wireless networks**” IEEE *Global Conference on Communication Technologies (GCCT-2015), Kanyakumari, 23rd-24th April 2015.*